020650 PCT/JP03/12022

19.09.03

REC'D 10 OCT 2003
WIPO PCT

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　９月２０日

出願番号
Application Number: 特願２００２－２７６３０６

[ST.10/C]: [ＪＰ２００２－２７６３０６]

出願人
Applicant(s): パイオニア株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２００３年　６月２６日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０５０５４０

【書類名】　特許願
【整理番号】　57P0255
【提出日】　平成14年 9月20日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/08
H04L 9/14
【発明者】
【住所又は居所】　埼玉県所沢市花園４丁目２６１０番地　パイオニア株式会社　所沢工場内
【氏名】　竹村　到
【発明者】
【住所又は居所】　埼玉県所沢市花園４丁目２６１０番地　パイオニア株式会社　所沢工場内
【氏名】　吉田　和幸
【特許出願人】
【識別番号】　000005016
【氏名又は名称】　パイオニア株式会社
【代理人】
【識別番号】　100107331
【弁理士】
【氏名又は名称】　中村　聡延
【電話番号】　03-5524-2323
【選任した代理人】
【識別番号】　100104765
【弁理士】
【氏名又は名称】　江上　達夫
【電話番号】　03-5524-2323
【手数料の表示】
【予納台帳番号】　131957

【納付金額】　　21,000円

【提出物件の目録】

【物件名】　　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【包括委任状番号】　0104687

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　鍵管理システム

【特許請求の範囲】

【請求項１】　複数の情報受信者をリーフに割り当てた木構造を規定する手段と、

前記木構造を所定階層毎に分割して複数の部分木を規定する手段と、

前記複数の部分木の各部分木に対して鍵情報の割り当てを行う手段と、

を有することを特徴とする鍵管理システム。

【請求項２】

前記鍵情報の割り当てを行う手段は、

前記部分木のリーフに割り当てられた複数の情報受信者全てにより構成される集合と、前記部分木中の特定のノード以下のリーフに割り当てられた情報受信者との差分集合を、前記部分木中の全てのノードについて特定する手段と、

前記差分集合の各々に鍵情報を割り当てる手段と、

前記複数の情報受信者の各々に対して、当該情報受信者が属する全ての差分集合に割り当てられた鍵情報を割り当てる手段と、

からなることを特徴とする請求項１記載の鍵管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、木構造を用い、特定の受信者の無効化機能を有する鍵管理方式に関する。

【０００２】

【従来の技術】

映画、音楽などの著作物であるコンテンツの著作権を保護するために、情報を利用してコンテンツを暗号化して提供することが行われている。そのようなシステムの一例では、再生装置には複数のデバイス鍵を与え、記録媒体には暗号化されたコンテンツと、再生を許可された再生装置のみがコンテンツの復号鍵を生成できるようにした鍵生成情報とを記録する。再生を許可された再生装置は、鍵生

成情報からコンテンツの復号鍵を生成し、その復号鍵を使用してコンテンツを復号して再生する。一方、再生を許可されていない（無効化された）再生装置は、コンテンツの復号鍵を生成できないので、暗号化されているコンテンツを再生することはできない。

【０００３】

このようなシステムで、鍵情報を管理するための手法として木構造を用いた鍵管理方式が提案されており、その例として「The Complete Subtree Method」、「The Subset Difference Method」などが知られている（例えば非特許文献１参照。）。これらの方式では、コンテンツの復号鍵を生成するための鍵生成情報が不正に暴露されたり漏洩した場合には、その鍵生成情報を無効化するための処理が可能となっている。

【０００４】

また、上記のような方式に基づいてデジタルコンテンツの保護を行う方法も提案されている（例えば非特許文献２参照。）。

【０００５】

【非特許文献１】

Dalit Naor, Noni Naor, and Heff Lotspiech,"Revocation and Tracing Schemes for Stateless Receivers", Lecture Notes in Computer Science, Vol.2139, pp.41-62, 2001

【非特許文献２】

中野稔久、他３名、“デジタルコンテンツ保護用鍵管理方式－木構造パターン分割方式－”、2002年暗号と情報セキュリティシンポジウム講演論文集、２００２年２月１日

【０００６】

【発明が解決しようとする課題】

上述のThe Subset Difference Methodにおいては、受信者は自分の属する全ての差分集合に割り当てられた鍵を保有しておかなければならないため、受信者側に多くの記憶容量を必要とする。疑似乱数生成器を用いることでこの情報量を削減することはできるのであるが、それでもThe Complete Subtree Methodと比較

すると１０倍以上の情報記憶容量が要求される。一方、The Complete Subtree Methodについては、受信者側に記憶すべき情報量は少ないが、受信者へ伝送される（情報の伝送に記録媒体を利用する場合には、記録媒体に記録される）鍵情報量が大きくなりすぎてしまう。本発明が解決しようとする課題には、上記のものが一例として挙げられる。

【０００７】

【課題を解決するための手段】

請求項１に記載の発明は、鍵管理システムにおいて、複数の情報受信者をリーフに割り当てた木構造を規定する手段と、前記木構造を所定階層毎に分割して複数の部分木を規定する手段と、前記複数の部分木の各部分木に対して鍵情報の割り当てを行う手段と、を有することを特徴とする。

【０００８】

【発明の実施の形態】

以下、図面を参照して本発明の好適な実施の形態について説明する。まず、鍵管理方式について基礎的な説明を行い、続いて本発明の方式を説明する。

【０００９】

（1.1）受信者の無効化機能を有する鍵管理方式

送信者が多数の受信者に対して同一の情報を伝送するシステムにおいて、信頼できる鍵管理機関が、あらかじめ全ての受信者に伝送情報を復号するための秘密情報を配布しておき、その秘密情報を持たない受信者が送信者からの情報を復号できないように、送信者側で情報を暗号化して伝送する方法がある。この場合に問題となるのは、全ての受信者が同一の秘密情報を保有している場合、悪意ある受信者が自分の保有する秘密情報を１回公開してしまえば、その後に伝送される情報は誰にでも復号が可能になってしまうことである。

【００１０】

この問題の対策として、鍵管理機関が受信者毎に異なる秘密情報を配布し、特定の受信者の秘密情報が漏洩した場合、その受信者の保有していた秘密情報を用いても伝送された情報を復号できないようにする手法、即ち、受信者の無効化機能を有する鍵管理方式がある。本発明はそのような鍵管理方式を扱う。

【００１１】

ここでは、情報の伝送は特定の送信者から多数の受信者への片方向伝送のみであり、また受信者に最初に秘密情報（復号鍵等）を割り当てる以外は、受信者の保有する秘密情報を一切変更できないようなアプリケーションを想定している。

【００１２】

受信者の無効化機能を有する鍵管理方式を適用した情報配信システムの１つのモデルを図１（ａ）に示す。図示のように、情報配信システムは、鍵管理機関１、情報送信者２及び情報受信者３の３つの要素から構成される。以下、各要素について説明する。

【００１３】

・鍵管理機関

鍵管理機関１は、情報送信者２が伝送する伝送情報６（暗号文）を復号するための秘密情報（暗号文復号用鍵４ａなど）を各受信者に割り当てる。また、鍵管理機関１は、伝送情報６を復号不可能にしたい受信者（今後、ある特定の受信者に対して、伝送される情報を復号できないようにすることを「受信者の無効化」と呼ぶ）の集合から、前記集合以外の受信者のみが復号できるような鍵情報４ｂを生成し、伝送情報６を暗号化するための鍵（暗号化用鍵情報５）とあわせて情報送信者への配送も行う。

【００１４】

ここで各受信者に割り当てる秘密情報（復号用鍵４ａなど）と伝送情報６の暗号化に用いられる鍵（暗号化用鍵情報５）の生成・保管・配送は安全に行われるものと仮定する。

【００１５】

・情報送信者

情報送信者２は、鍵管理機関１から配送された、伝送情報の暗号化用鍵情報５を用いて伝送情報６を暗号化し、無効化されていない受信者のみが復号できる鍵情報４ｂと一緒に伝送情報６（暗号文）を受信者に伝送する。

【００１６】

・情報受信者

無効化されていない受信者については、伝送情報６（暗号文）を受信したとき、受信者が持つ秘密情報（暗号文復号用の鍵４ａ等）を使って受信した鍵情報４ｂを復号し、復号された鍵を用いて暗号文から伝送情報６を復号する。逆に無効化されている受信者については、そのような受信者が複数結託しても、伝送情報に関して何の情報も得られない。また、ここでは多数の受信者の存在を想定している。

【００１７】

以下、上記構成要素について詳しく説明する。

【００１８】

$\underline{N}$を全ての受信者の集合とし、その要素数を$|\underline{N}|=N$とする。$\underline{N}$の部分集合$\underline{R}$を無効化したい受信者の集合とし、その要素数を$|\underline{R}|=r$とする。受信者の無効化機能を有する鍵管理方式の目的は、鍵管理機関（又は情報送信者）が受信を許可した受信者、つまり$\underline{R}$に含まれない全ての受信者$u\in\underline{N}\setminus\underline{R}$が伝送される情報を復号でき、逆に受信を許可されていない$\underline{R}$に含まれる受信者全てが結託しても全く伝送情報を得られないようにすることである。

【００１９】

(a)鍵管理機関

（i）初期設定

受信者全体の集合$\underline{N}$の部分集合$\underline{S}_1$、$\underline{S}_2$、・・・、$\underline{S}_w$（$\forall j$、$\underline{S}_j\subseteq\underline{N}$）を定義する。各$\underline{S}_j$には暗号（復号）鍵$L_j$が割り当てられる。ここで各$L_j$は一様に分布しており、互いに独立な値を割り当てるのが望ましい。各受信者（受信装置）ｕには、秘密情報I_uを割り当てる。ここで$\underline{S}_j$に含まれる全ての受信者$u\in\underline{S}_j$が、自分に割り当てられた秘密情報I_uから、自分の属する部分集合$\underline{S}_j$に割り当てられた復号鍵L_jを求められるように秘密情報I_uを割り当てなければならない。また、$\underline{S}_j$に含まれない全ての受信者$u\in\underline{N}\setminus\underline{S}_j$が結託しても復号鍵$L_j$を求めることができないように秘密情報$I_u$を割り当てなければならない。

【００２０】

（ii）鍵情報生成

(1)伝送情報Ｍの暗号化、復号化に用いる鍵（セッション鍵）Ｋを選ぶ。

【００２１】

(2)無効化する受信者の集合Ｒの補集合Ｎ＼Ｒに属する受信者ｕ∈Ｎ＼Ｒをいくつかの部分集合S_{i1}、S_{i2}、・・・、S_{im}に分割する。

【００２２】

【数１】

$$\mathcal{N} \setminus \mathcal{R} = \bigcup_{j=1}^{m} S_{i_j} \qquad (1\text{-}1)$$

【００２３】

ここで、初期設定で上記部分集合に割り当てられてた暗号鍵をそれぞれL_{i1}、L_{i2}、・・・L_{im}とする。

【００２４】

(3)暗号鍵L_{i1}、L_{i2}、・・・L_{im}を用いてセッション鍵Ｋをｍ回暗号化して式（1-2）を生成、セッション鍵Ｋと一緒に情報送信者に配送する。

【００２５】

【数２】

$$\langle i_1, i_2, \cdots, i_m, E_{enc}(K, L_{i_1}), E_{enc}(K, L_{i_2}), \cdots, E_{enc}(K, L_{i_m}) \rangle \qquad (1\text{-}2)$$

【００２６】

ここで、情報送信者へのセッション鍵の配送は安全に行われるものと仮定する。また、E_{enc}は暗号化アルゴリズムである。本システムで用いられる暗号、復号化アルゴリズムは２種類あり、以下にまとめる（ただし、２つのアルゴリズムに全く同じものを使用しても構わない）。

【００２７】

・伝送情報Ｍの暗号化アルゴリズムF_{enc}、復号化アルゴリズムF_{dec}

セッション鍵Ｋを用いて暗号文$C_K = F_{enc}$（Ｍ、Ｋ）を生成する。高速性が要求される。

【００２８】

・セッション鍵暗号化アルゴリズムE_{enc}、復号化アルゴリズムE_{dec}

セッション鍵の配送に用いる。F_{enc}よりも暗号化アルゴリズムの安全性が要求される。

【００２９】

（ｂ）情報送信者

セッション鍵Ｋと特定の受信者のみが復号できる鍵情報を鍵管理機関から受け取り、セッション鍵Ｋを鍵として暗号化アルゴリズムF_{enc}を用いて伝送情報Ｍを暗号化して、暗号文

【００３０】

【数３】

$$\langle [i_1, i_2, \cdots, i_m, E_{enc}(K, L_{i_1}), E_{enc}(K, L_{i_2}), \cdots, E_{enc}(K, L_{i_m})], F_{enc}(M, K) \rangle \qquad (1\text{-}3)$$

【００３１】

を伝送する。なお、式（1-3）の［　］内の部分をF_{enc}（Ｍ、Ｋ）のヘッダーと呼ぶことにする。

【００３２】

（ｃ）情報受信者

受信者ｕは、情報送信者により暗号化された次の暗号文を受信する。

【００３３】

【数４】

$$\langle [i_1, i_2, \cdots, i_m, C_1, C_2, \cdots, C_m], C_K \rangle \qquad (1\text{-}4)$$

【００３４】

(1) $u \in \underline{S}_{ij}$であるようなi_jを探索する。（$u \in \underline{R}$の場合、存在しない。）

(2) 自身の保有する秘密情報I_uからL_{ij}を求める。

【００３５】

(3) $K = E_{dec}$（C_j、L_{ij}）を求める。

【００３６】

(4)$M = F_{dec}(C_K, K)$を求める。

【００３７】

上記鍵管理方式を実現するアルゴリズムとして以下の方式がある。

・The Logical Key Hierarchy Method

・CPRM Common Cryptographic Key Management

・The Complete Subtree Method

・The Subset Difference Method

・Tree Pattern Division Method

上記方式の違いとしては、(1) 受信者の部分集合S_1、・・・、S_wの定義、(2) 各部分集合に対する鍵の割り当て方法、(3) 受信を許可する（無効化しない）受信者の集合N＼Rの分割方法、(4)各受信者uが行う自分の属する部分集合S_jの探索方法と、I_uから鍵L_{Sj}の求め方等が挙げられる。

【００３８】

各方式は以下の３つの観点から評価される。

【００３９】

・伝送情報の量

暗号文$F_{enc}(M, K)$に付加されるヘッダー量。一般にN＼Rを分割した部分集合の数mに比例する。

【００４０】

・受信者が保有しておく秘密情報I_uの量

復号用の鍵等の秘密情報を受信者がどれだけ保持しておかなければならないか。

【００４１】

・受信者が伝送された情報を復号するのに要する演算量

(1.2)　基礎となる方法 (The Subset Difference Method)

(1.2.1)　部分集合S_1、・・・S_wの定義

最初に受信者全体の集合Nの部分集合S_1、・・・S_wを定義する。この部分集合に対して暗号（復号）鍵、又は復号鍵を導けるような情報L_1、・・・L_wを割り当てることになる。Ｎ枚のリーフを持つ２分木のリーフに各受信者を割り当て

る（ここでＮは２の冪であるとしている。）。

【００４２】

受信者の部分集合を次のように表す。２分木中の任意のノードv_i（ルートとリーフもノードに含まれる。）をルートとする部分木の全てのリーフに割り当てられた受信者の集合をS_iで表す。任意のノードv_i以下のリーフに割り当てられた受信者の集合S_iとノードv_iをルートとする部分木中の（ルートを除く）ノードv_jをルートとする部分木の全てのリーフに割り当てられた受信者の集合$S_j \subset S_i$について、S_iの要素からS_jの要素を引いた差分集合を$S_{i,j}$とする。つまり、集合S_iに含まれる受信者のうち、集合S_jに含まれていない受信者の集合を$S_{i,j}$とする。図２は$S_{i,j}$を示している。この差分集合に対して１つの鍵$L_{i,j}$を割り当てる。

【００４３】

(1.2.2)　Ｎ＼Ｒの分割方法

次に受信を許可する（無効化しない）受信者の集合Ｎ＼Ｒを、上記で定義された差分集合$S_{i1,j1}$、$S_{i2,j2}$、・・・、S_{imjm}に分割する方法を説明する。２分木のルートと無効化したい受信者に相当する各リーフを結ぶ最短のパス上のノードのみで構成される部分木ＳＴ（Ｒ）を考える（このような部分木はＲから一意に構成される）。ＳＴ（Ｒ）については子ノードの存在しないノードをリーフと呼ぶことにする。以下のアルゴリズムをＳＴ（Ｒ）がルートのノードのみになるまで繰り返し、Ｎ＼Ｒを構成する差分集合を選択する。

【００４４】

(1) ２つのリーフからルートへのパスの共通部分に存在するノードの中で、リーフとの距離が最小となるノードを２つのリーフの最小共通ノードと呼ぶことにする。ＳＴ（Ｒ）のリーフv_i、v_jを、それらの最小共通ノードｖ以下に他のリーフが存在しないように選ぶ。ｖの２つの子ノードの中で、ｖとv_iのパス上に存在する子ノードをv_k、ｖとv_jのパス上に存在する子ノードをv_lとする。（リーフがＳＴ（Ｒ）中に１つしか存在しない場合、$v_i = v_j$、$v = v_l = v_k$として、ｖをＳＴ（Ｒ）のルートと考えればよい。）

(2) $v_k \neq v_i$ならば、Ｎ＼Ｒを構成する差分集合に$S_{k,i}$を加える。$v_l \neq v_j$な

らば$\underline{N} \setminus \underline{R}$を構成する差分集合に$\underline{S}_{1,j}$を加える。

【００４５】

(3) ｖより下に位置するノードを全て除去する。これによりｖがリーフになる。

【００４６】

上記アルゴリズムを用いることにより、受信者の集合$\underline{N} \setminus \underline{R}$は、無効化したい受信者数$|\underline{R}|$＝ｒのとき、最大 ２ｒ－１の差分集合に分割される。

【００４７】

(1.2.3) 部分集合$\underline{S}_1$、・・・$\underline{S}_w$への鍵の割り当て方法

次に、各差分集合に対する鍵の割り当て方法について説明する。各差分集合に対して、一様に分布しており、互いに独立な値を持つ鍵を割り当てる。

【００４８】

(1.2.4) 受信者への秘密情報の割り当て方法

各受信者には自分の属する差分集合全ての鍵を配布しておかなければならない。これは受信者側に非常に多くの記憶量を必要とする。受信者ｕは、自分の属する各部分木T_kに対して（ここでT_kの変数ｋは部分木の高さを表している。）、部分木T_k中に存在するノードの中で、T_kのルートからｕのパス上に存在するものを除く全てのノードの数に相当する鍵を保有しなければならない。受信者ｕの属する部分木の数は$\log_2 N$個存在し、各部分木の高さは$1 \leqq k \leqq \log_2 N$であるから、受信者が保有しなければならない鍵の数は式（2-1）のようになる。

【００４９】

【数５】

$$1 + \sum_{k=1}^{\log_2 N} (2^{k+1} - k - 2) \qquad (2\text{-}1)$$

【００５０】

(1.2.5) 部分集合$\underline{S}_1$、・・・、$\underline{S}_w$への鍵の割り当て方法（擬似乱数生成器を用いる場合）

受信者が保有しておく鍵を減らすため、各差分集合$\underline{S}_{i,j}$に直接鍵を割り当て

るのではなく、部分集合$\underline{S}_i$に対して１つのラベルを割り当て、差分集合$\underline{S}_{i,j}$（$\forall j$、$\underline{S}_j \subset \underline{S}_i$）に割り当てる鍵$L_{i,j}$が、部分集合$\underline{S}_i$に割り当てられたラベルを用いて導けるようにしておく。このとき、差分集合$\underline{S}_{i,j}$内に存在する受信者のみが鍵$L_{i,j}$を導けるようにしなければならない。以下では、擬似乱数生成器を用いて、上記方法を実現する方法を示す。

【００５１】

$G:\{0,1\}^n \rightarrow \{0,1\}^{3n}$ を入力長の３倍の長さを出力する擬似乱数生成器とする。擬似乱数生成器Ｇの入力をＳとしたとき、出力される値を３等分した左側部分をG_L（Ｓ）で表し、右側部分をG_R（Ｓ）、中央部分をG_M（Ｓ）で表す。また、Ｇの入力として乱数を与えたときに出力される値と、出力と同じ長さの真の乱数を多項式時間の計算能力をもつ攻撃者に与えたとき、攻撃者は、有意な確率で両者を区別できないといった特性をＧは満たしていなければならない。

【００５２】

ノードv_iをルートとする部分木T_iを考える。ノードv_iにラベル $LABEL_i$を割り当てる（簡単のため任意の部分木のリーフに割り当てられた受信者の集合へのラベルの割り当てを、その部分木のルートノードにラベルを割り当てると表現する。つまり上記表現は次のようになる。「部分木T_i中のリーフに割り当てられた受信者の集合$\underline{S}_i$にラベル$LABEL_i$を割り当てる。」）。$LABEL_{i,j}$を、部分木T_i中のノードv_jのラベルとする（割り当てられるラベルが多変数のパラメータを持つ（この場合ｉとｊの２変数）場合、それは差分集合に対して割り当てられたラベルを示している。このとき、$LABEL_{i,j}$は v_jをルートとする部分木のリーフに割り当てらた受信者の集合$\underline{S}_j$に割り当てられるのではなく、$\underline{S}_i$に含まれ、$\underline{S}_j$には含まれていない受信者の集合（差分集合）$\underline{S}_{i,j}$に対して割り当てられる。）。$LABEL_{i,j}$が差分集合$\underline{S}_{i,j}$に割り当てられるラベルである。

【００５３】

$LABEL_{i,j}$を部分木T_iのルートv_iに割り当てられたラベル$LABEL_i$から擬似乱数生成器Ｇを用いて以下の導出規則により導く。ラベルを擬似乱数生成器の入力としたとき、その出力を次のように定義する。G_L－左側の子ノードのラベル、G_R

－右側の子ノードのラベル、G_M－入力ラベルの割り当てられたノードに割り当てる暗号（復号）鍵。この導出規則に拠れば、部分木T_i中のある親ノードにラベルＳが割り当てられたとき、その２つの子ノードのラベルは、G_L（Ｓ）、G_R（Ｓ）が割り当てられる。これより、v_iからv_jに至るパス上のノードに割り当てるラベルをＧを用いて順次求めることで、v_iに割り当てられたラベル$LABEL_i$から、部分木T_i中のノードv_jのラベル $LABEL_{i,j}$を求めることができる。

【００５４】

最後に$LABEL_{i,j}$をＧの入力としたときの出力の中央部分G_M（$LABEL_{i,j}$）を、差分集合$\underline{S}_{i,j}$に割り当てる暗号（復号）鍵$L_{i,j}$として用いる。図３（ａ）に部分木T_i中のノードv_jに割り当てるラベルと暗号（復号）鍵の生成方法を示す。

【００５５】

このような方法を用いれば、部分木中のあるノードのラベルが与えられたとき、その子孫ノード全てのラベルと暗号（復号）鍵を計算することができる。逆に、あるノードv_jの先祖ノードのラベルをv_jから求めることはできない。さらに、ノードv_jの全ての子孫ノードのラベル（ただし、v_j自身のラベルは含まない）から暗号（復号）鍵$L_{i,j}$を求めることはできない。部分木T_iのルートのラベル$LABEL_i$を与えられたとき、差分集合$\underline{S}_{i,j}$に割り当てられる暗号（復号）鍵$L_{i,j}$を計算するのに擬似乱数生成器Ｇを最大で$\log_2 N+1$回用いる。

【００５６】

（1.2.6）受信者への秘密情報の割り当て方法（擬似乱数生成器を用いる場合）

各受信者ｕが保有する秘密情報I_uの割り当て方法について説明する。受信者ｕは、自分の属する各部分木T_iに対して、T_iのルートノードv_iと、部分木T_i中のノードでｕの先祖ノードでない全てのノードv_iにより決定される差分集合$S_{i,j}$に割り当てられた暗号（復号）鍵$L_{i,j}$を計算できなければならない。部分木T_iのルートノードv_iからｕへのパスを考え、そのパスに直接ぶら下がるノードをv_{i1}、v_{i2}、・・・v_{ik}とする（図２（ｂ）参照）。つまり、それらはパスに隣接するノードの中で、ｕの先祖ノードでないノードである。部分木T_i中でｕの先祖でない任意のノードv_iは、これらのノードv_{i1}、v_{i2}、・・・、v_{ik}

いずれかの子孫ノードである。ゆえに、受信者ｕがI_uとして、v_{i1}、v_{i2}、・・・、v_{ik}に割り当てられたラベルを保有しておけば、最大$\log_2 N+1$回擬似乱数生成器Ｇを用いて、部分木T_i中でパス上に存在しない任意ノードv_{ij}に割り当てられた復号鍵$L_{i,j}$を計算することができる。

【００５７】

受信者ｕを含む高さｋの部分木T_i中に、受信者ｕが保存しておかなければならないラベルはｋ個あるから、これをｕを含む各部分木について考えると、受信者ｕがあらかじめ保有しておかなければならない復号鍵（ラベル）の数は式（2-2）のようになる。

【００５８】

【数６】

$$1+\sum_{k=1}^{\log_2 N} k = 1+\frac{(1+\log_2 N)\log_2 N}{2} = \frac{1}{2}(\log_2 N)^2+\frac{1}{2}\log_2 N+1 \qquad (2\text{-}2)$$

【００５９】

式（2-2）で１が足されているのは、無効化する受信者が全く存在しない場合の鍵が必要だからである。

【００６０】

（1.2.7）複数の２分木を用いる方法

さらに受信者ｕが保有する秘密情報I_uを減らす場合は、伝送情報Ｍの量とのトレードオフとなる。一つの方法として、２分木を高さの低い木に限定して複数用いる方法がある。木構造においてノードの位置する各層をレイヤと呼び、ルートの位置する層から順番に Layer(0)、Layer(1)、・・・と定義する。このとき、受信者をリーフに割り当てられた２分木を、Layer(b) に存在するノードをルートとする2^b個の２分木に分割し、分割された２分木に対して The Subset Difference Method を適用する。このとき、Layer(0)～Layer(b-1)に存在するノードは使用しない。

【００６１】

これにより、受信者が保有しておく情報量I_uを式（2-3）のように減らすこと

ができる。しかし、伝送情報Ｍの量（無効化しない受信者をカバーする部分木の数）は、無効化したい受信者数を｜Ｒ｜＝ｒとすると最大で2^b+2r-1と増加する。

【００６２】

【数７】

$$1+\sum_{k=1}^{\log_2 N-b} k=\frac{1}{2}(\log_2 N-b)^2+\frac{1}{2}(\log_2 N-b)+1 \qquad (2\text{-}3)$$

【００６３】

（1.3）本実施形態による方法（The Layer Division Subset Difference Method）

（1.3.1）部分集合S_1、・・・、S_Wの定義

最初に受信者全体の集合Ｎの部分集合S_1、・・・S_Wを定義する。この部分集合に対して暗号（復号）鍵、又は復号鍵を導けるような情報L_1、・・・L_Wを割り当てることになる。Ｎ枚のリーフを持つ２分木のリーフに各受信者を割り当てる（ここでＮは２の冪であるとしている。）。木構造においてノードの位置する各層をレイヤと呼び、ルートの位置する層から順番に Layer(0)、Layer(1)、・・・と定義する。リーフの存在する層は Layer($\log_2$N)になる。図４に示すように２分木をLayer(0)～Layer(d)、Layer(d)～Layer(2d)、・・・といったようにd+1階層ずつのレイヤに分割する。図４ではd=2の場合を示している。分割された各層をマクロレイヤと呼ぶことにし、ルートを含むマクロレイヤから順番に MacroLayer(0)、MacroLayer(1)、・・・、MacroLayer（($\log_2$N)/d－１）と定義する。各MacroLayer(s)(0≦s≦（($\log_2$N)/d－１）)は、全体の２分木を分割した高さdの2^{sd}個の部分木T_hから構成される。全体で上記部分木T_hは

【数８】

$$(1-2^{\log_2 N})/(1-2^d)$$

個存在することになる。各部分木

【数９】

$$T_h (0 \leq h \leq (2^d - 2^{\log_2 N})/(1-2^d))$$

を、リーフに受信者を割り当てた２分木と考え、The Subset Difference Method において定義された差分集合を部分集合$\underline{S}_1$、・・・$\underline{S}_W$として定義し、暗号（復号）鍵L_1、・・・L_Wを割り当てる。（実際には、部分木T_hのリーフは、s=($\log_2 N$)/d-1の場合（MacroLayer(($\log_2 N$)/d-1)中の部分木）を除いて、全体の２分木で見た場合ただのノードであり、受信者が割り当てられているわけではない。そこで、ある任意の部分木T_hにおけるリーフには、そのリーフに対応する全体の２分木中のノード以下に存在する全てのリーフに割り当てられた受信者の集合が割り当てられていると考える。）。

【００６４】

部分木T_h中の任意のノードv_iをルートとする部分木$T_{h,i}$の全てのリーフに割り当てられた受信者の集合を$\underline{S}_i$で表す。ノードv_i以下のリーフに割り当てられた受信者の集合$\underline{S}_i$と$T_{h,i}$中の（ルートを除く）ノードv_jをルートとする部分木$T_{h,j}$のリーフに割り当てられた受信者の集合$\underline{S}_j \subset \underline{S}_i$について、$\underline{S}_i$の要素から$\underline{S}_j$の要素を引いた差分集合を$\underline{S}_{i,j}$とする。つまり、集合$\underline{S}_i$に含まれる受信者のうち、集合$\underline{S}_j$に含まれていない受信者の集合を$\underline{S}_{i,j}$とする。図５は$\underline{S}_{i,j}$を示している。この差分集合に対して１つの暗号（復号）鍵$L_{i,j}$を割り当てる。

【００６５】

(1.3.2) $\underline{N} \setminus \underline{R}$の分割方法

次に受信を許可する（無効化しない）受信者の集合$\underline{N} \setminus \underline{R}$を、上記で定義された差分集合$\underline{S}_{i,j}$に分割する方法を説明する。無効化したい受信者を割り当てられているリーフ、または無効化したい受信者を１つでも含むような受信者の集合を割り当てられているリーフを含む全ての部分木T_hについて以下の処理を行う。

【００６６】

無効化したい受信者を含む部分木T_hについて、部分木T_hのルートと無効化し

たい受信者（又は無効化したい受信者を含む受信者の集合）に相当する各リーフを結ぶ最短のパス上のノードのみで構成される部分木$ST_h(\underline{R})$を考える（このような部分木は$\underline{R}$から一意に構成される）。$ST_h(\underline{R})$については子ノードの存在しないノードをリーフと呼ぶことにする。また、以下の(1)～(4)の処理において用いられているルートとリーフは、部分木T_h中のそれを表しているものとする。

【００６７】

(1) ２つのリーフからルートへのパスの共通部分に存在するノードの中で、リーフとの距離が最小となるノードを２つのリーフの最小共通ノードと呼ぶことにする。$ST_h(\underline{R})$のリーフv_i、v_jを、それらの最小共通ノードｖ以下に他のリーフが存在しないように選ぶ。ｖの２つの子ノードの中で、ｖとv_iのパス上に存在する子ノードをv_k、ｖとv_jのパス上に存在する子ノードをv_lとする。（リーフが$ST_h(\underline{R})$中に１つしか存在しない場合、$v_i=v_j$、$v=v_j=v_k$として、ｖを$ST_h(R)$のルートと考えればよい。）

(2) $v_k \neq v_i$ならば$\underline{N} \setminus \underline{R}$を構成する差分集合に$\underline{S}_{k,i}$を加える。$v_l \neq v_j$ならば$\underline{N} \setminus \underline{R}$を構成する差分集合に$\underline{S}_{l,j}$を加える。

【００６８】

(3) ｖより下に位置する部分木T_h中のノードを全て除去する。これにより、ｖがリーフになる。

【００６９】

(4) $ST_h(\underline{R})$にルート以外のノードが存在する場合、上記(1)に戻る。$ST_h(\underline{R})$がルートのノードのみなった場合、無効化したい受信者を含む他の部分木T_hを選択し、上記(1)に戻って同様の処理を繰り返す。$ST_h(\underline{R})$がルートのノードのみなり、かつ無効化したい受信者を含む他の部分木T_hが存在しない場合、処理を終了する。

【００７０】

上記アルゴリズムにより構成された差分集合$\underline{S}_{i,j}$の集合が$\underline{N} \setminus \underline{R}$を構成する差分集合の集合である。$\underline{N} \setminus \underline{R}$の分割数（$\underline{N} \setminus \underline{R}$を構成する差分集合の数）の上限は、ｄの値により異なるが、例えばd=2のとき（このとき、Ｎは４の冪である

と仮定している。）、無効化したい受信者数｜R｜＝ｒとすると式（3-1）のようになる。

【００７１】

【数１０】

$$1+\sum_{j=1}^{r} f_j \qquad (3\text{-}1)$$

$$f_j=\begin{cases}\log_4(N)-1 & (j=1)\\ \log_4(N) & (j=2)\\ \log_4(N/4^i) & (2\cdot 4^{i-1}<j\le 4^i)\\ \log_4(N/4^i)-1 & (4^i<j\le 2\cdot 4^i \text{ かつ } j \text{が奇数})\\ \log_4(N/4^i) & (4^i<j\le 2\cdot 4^i \text{ かつ } j \text{が偶数})\\ -1 & (2\cdot 4^{\log_4 N-1}<j\le 4^{\log_4 N}=N)\end{cases}$$

【００７２】

ここでiは$0<i<\log_4 N$を満たす整数である。

【００７３】

（1.3.3）部分集合$\underline{S}_1$、・・・、$\underline{S}_W$への鍵の割り当て方法

次に各差分集合に対する鍵の割り当て方法について説明する。各差分集合$\underline{S}_{i,j}$に対して、一様に分布しており、互いに独立な値を持つ鍵を割り当てる。各受信者には自分の属する差分集合に割り当てられた全ての鍵を配布しておく。

【００７４】

（1.3.4）受信者への秘密情報の割り当て方法

受信者ｕを割り当てられたリーフと、全体の２分木のルートとのパス上に存在するノードを含む各部分木T_hについて考える。このような部分木T_hは各マクロレイヤ中に必ず１つ存在する。パス上のノードの中で部分木T_hに含まれる任意のノードをv_iとし、v_iをルートとする部分木$T_{h,i}$のリーフに割り当てられた受信者の集合を$\underline{S}_i$とする。部分木$T_{h,i}$中のノードであり、かつパス上に存在しないノードをv_jとし、v_jをルートとする部分木$T_{h,j}$のリーフに割り当てられた受信者の集合を$\underline{S}_i \subset \underline{S}_j$とする。集合$\underline{S}_i$に含まれ、集合$\underline{S}_j$に含まれない受信者の集合（差分集合）を$\underline{S}_{i,j}$で表す。このとき受信者ｕは上記の全ての差分集合$\underline{S}_{i,j}$に割り当てられた鍵を保有しておく必要がある。受信者ｕの属する部分

木T_hの数は、マクロレイヤ数に等しいから$\log_2 N$／d個存在する。部分木T_hの高さはdであるから、部分木T_h中に存在し、かつパス上のノードv_iをルートとする部分木$T_{h,i}$はd個存在する（ノードv_iが部分木T_hのリーフに相当する場合は、受信者の集合を割り当てる必要がないため除外している。）。部分木$T_{h,i}$の高さをk、（$1 \leqq k \leqq d$）とすると、部分木$T_{h,i}$中のノードで、かつパス上に存在しないノードv_jをルートとする部分木$T_{h,j}$は｛$(2^{k+1}-1)-(k+1)$｝個存在する。これより各部分木$T_{h,i}$について、集合$\underline{S}_j$の数は｛$(2^{k+1}-1)-(k+1)$｝個である。よって差分集合$\underline{S}_{i,j}$の数は式（3-2）のようになる。受信者uは式（3-2）に示すだけの個数の鍵を保有しておかなければならない。式（3-2）において1が足されているのは、無効化する受信者が全く存在しない場合の鍵が必要だからである。

【００７５】

【数１１】

$$1+\frac{\log_2 N}{d}\sum_{k=1}^{d}(2^{k+1}-k-2)=\frac{4(2^d-1)\log_2 N}{d}-\frac{(d+5)\log_2 N}{2}+1 \qquad (3\text{-}2)$$

【００７６】

（1.3.2）部分集合$\underline{S}_1$、・・・、$\underline{S}_W$への鍵の割り当て方法（擬似乱数生成器を用いる場合）

受信者が保有しておく鍵を減らすため、The Subset Difference Method と同様に擬似乱数生成器を用いて差分集合への鍵の割り当てを行うこともできる。つまり、各差分集合$\underline{S}_{i,j}$に直接鍵を割り当てるのではなく、部分木$T_{h,i}$のリーフに割り当てられた受信者の集合$\underline{S}_i$に対して１つのラベルを割り当てる。このとき、差分集合$\underline{S}_{i,j}$（$^{\forall}$j、$\underline{S}_j \subset \underline{S}_i$）に割り当てる鍵$L_{i,j}$が、部分集合$\underline{S}_i$に割り当てられたラベルを用いて導けるようにしておく。このとき、差分集合$\underline{S}_{i,j}$内に存在する受信者のみが鍵$L_{i,j}$を導けるようにしなければならない。以下では、擬似乱数生成器を用いて、上記方法を実現する方法を示す。

【００７７】

$G:\{0,1\}^n \rightarrow \{0,1\}^{3n}$ を入力長の３倍の長さを出力する擬似

乱数生成器とする。擬似乱数生成器Ｇの入力をＳとしたとき、出力される値を３等分した左側部分を G_L（Ｓ）で表し、右側部分をG_R（Ｓ）、中央部分をG_M（Ｓ）で表す。また、Ｇの入力として乱数を与えたときに出力される値と、出力と同じ長さの真の乱数を多項式時間の計算能力をもつ攻撃者に与えたとき、攻撃者は、有意な確率で両者を区別できないといった特性をＧは満たしていなければならない。

【００７８】

ノードv_iをルートとするMacroLayer(s)中の部分木$T_{h,i}$を考える。ルートノードv_iにラベル$LABEL_i$を割り当てる（簡単のため任意の部分木のリーフに割り当てられた受信者の集合へのラベルの割り当てを、その部分木のルートノードにラベルを割り当てると表現する。つまり上記表現は次のようになる。「部分木$T_{h,i}$中のリーフに割り当てられた受信者の集合$\underline{S}_i$にラベル $LABEL_i$を割り当てる。」）。$LABEL_{i,j}$を、部分木$T_{h,i}$中のノードv_jのラベルとする（割り当てられるラベルが２変数のパラメータを持つ場合、それは差分集合に対して割り当てられたラベルを示している。このとき、$LABEL_{i,j}$はv_jをルートとする部分木のリーフに割り当てらた受信者の集合$\underline{S}_j$に割り当てられるのではなく、$\underline{S}_i$に含まれ、$\underline{S}_j$には含まれていない受信者の集合（差分集合）$\underline{S}_{i,j}$に対して割り当てられる。）。$LABEL_{i,j}$が差分集合$\underline{S}_{i,j}$に割り当てられるラベルである。$LABEL_{i,j}$を部分木$T_{h,i}$のルートv_iに割り当てられたラベル$LABEL_i$から擬似乱数生成器Ｇを用いて以下の導出規則により導く。

【００７９】

ラベルを擬似乱数生成器の入力としたとき、その出力を次のように定義する。G_L－左側の子ノードのラベル、G_R－右側の子ノードのラベル、G_M－入力ラベルの割り当てられたノードに割り当てる暗号（復号）鍵。この導出規則に拠れば、部分木$T_{h,i}$中のある親ノードにラベルＳが割り当てられたとき、その２つの子ノードのラベルは、G_L（Ｓ）、G_R（Ｓ）が割り当てられる。これより、v_iからv_jに至るパス上のノードに割り当てるラベルをＧを用いて順次求めることで、v_iに割り当てられたラベル$LABEL_i$ から、部分木$T_{h,i}$中のノードv_jのラベル$LABEL_{i,j}$を求めることができる。最後に$LABEL_{i,j}$をＧの入力としたときの出力

の中央部分$G_M(LABEL_{i,j})$を、差分集合$\underline{S}_{i,j}$に割り当てる暗号（復号）鍵$L_{i,j}$として用いる。図６に差分集合$\underline{S}_{i,j}$に割り当てる鍵$L_{i,j}$の割り当て例を示す。

【００８０】

このような方法を用いれば、部分木中のあるノードのラベルが与えられたとき、部分木内でのその子孫ノード全てのラベルと暗号（復号）鍵を計算することができる。逆に、あるノードv_jの先祖ノードのラベルをv_jから求めることはできない。さらに、ノードv_jの全ての子孫ノードのラベル（ただし、v_j自身のラベルは含まない）から暗号（復号）鍵$L_{i,j}$を求めることはできない。部分木$T_{h,i}$のルートのラベル$LABEL_i$を与えられたとき、差分集合$\underline{S}_{i,j}$に割り当てられる暗号（復号）鍵$L_{i,j}$を計算するのに擬似乱数生成器Ｇを最大でd+1回用いる。

【００８１】

（1.3.6）受信者への秘密情報の割り当て方法（擬似乱数生成器を用いる場合）

各受信者ｕが保有する秘密情報I_uの割り当て方法について説明する。各マクロレイヤ中に１つずつ存在するｕの属する部分木T_hについて考える。部分木T_hのルートとｕの割り当てられたリーフを結ぶパス上のｄ個（リーフ部分のノードは数えていない。）のノードをv_iとし、v_iをルートとする高さｋ、（$1 \leqq k \leqq d$）の部分木$T_{h,i}$のノードの中で、パスに直接ぶら下がるノードをv_{i1}、v_{i2}、・・・v_{ik}で表す（図７）。つまり、それらは部分木$T_{h,i}$中のノードの中で、パスに隣接し、かつｕの先祖ノードでないノードである。部分木$T_{h,i}$中のノードで、ｕの先祖でない任意のノードv_jは、これらのノードv_{i1}、v_{i2}、・・・v_{ik}のいずれかの子孫ノードである。ゆえに、受信者ｕがI_uとして、v_{i1}、v_{i2}、・・・、v_{ik}に割り当てられたラベルを保有しておけば、最大d+1回擬似乱数生成器Ｇを用いて、部分木$T_{h,i}$中でパス上に存在しない任意ノードv_jに割り当てられた復号鍵$L_{i,j}$を計算することができる。

【００８２】

受信者ｕを含む部分木T_hの数は、マクロレイヤ数に等しいから$\log_2 N/d$であり、部分木T_h中にパス上のノードをルートとする部分木$T_{h,i}$はｄ個存在する。高さｋの部分木$T_{h,i}$中に受信者ｕが保有しなければならないラベルはｋ個ある

から、これをｕを含む各部分木$T_{h,i}$について考えると、受信者ｕが保有しておかなければならない復号鍵（ラベル）の数は式（3-3）のようになる。

【００８３】

【数１２】

$$1+\frac{\log_2 N}{d}\sum_{k=1}^{d}k=\frac{(d+1)\log_2 N}{2}+1 \qquad (3\text{-}3)$$

【００８４】

式（3-3）において１が足されているのは、式（3-2）と同様に無効化する受信者が全く存在しない場合の復号鍵が必要だからである。擬似乱数生成器を用いて差分集合への鍵の割り当てを行った場合、受信者の保有する秘密情報は復号鍵ではなく各部分木$T_{h,i}$に割り当てられたラベルであるが、受信者を全く無効化しない場合に用いる復号鍵については鍵そのものを保有することになる。

【００８５】

（1.3.7）複数の２分木を用いる方法

さらに受信者ｕが保有する秘密情報I_uを減らす場合は、伝送情報Ｍの量とのトレードオフとなる。一つの方法として、２分木を高さの低い木に限定して複数用いる方法がある。受信者をリーフに割り当てられた２分木を、Layer(b)に存在するノードをルートとする2^b個の２分木に分割し、分割された２分木に対して本方式を適用する。このとき、Layer(0) ～ Layer(b-1)に存在するノードは使用しない。これにより、受信者が保有しておく情報量I_uを式（3-4）、式（3-5）のように減らすことができる。擬似乱数生成器を用いない場合の復号鍵（ラベル）保有数が、式（3-4）であり、擬似乱数生成器を用いる場合のそれが式（3-5）である。式（3-4）、式（3-5）において共に１が足されているのは、自身の割り当てられているリーフの属する２分木中に、無効化する受信者が全く存在しない場合の鍵が必要だからである。

【００８６】

【数１３】

$$1+\frac{\log_2 N-b}{d}\sum_{k=1}^{d}(2^{k+1}-k-2)=\frac{4(2^d-1)(\log_2 N-b)}{d}-\frac{(d+5)(\log_2 N-b)}{2}+1 \qquad (3\text{–}4)$$

$$1+\frac{\log_2 N-b}{d}\sum_{k=1}^{d}k=\frac{(d+1)(\log_2 N-b)}{2}+1 \qquad (3\text{–}5)$$

【００８７】

伝送情報Ｍの量（無効化しない受信者をカバーする部分木の数）の上限は、例としてd=2のときを考えると、無効化したい受信者数が｜Ｒ｜＝ｒのとき式（3–6）のようになる。

【００８８】

【数１４】

$$4^h+\sum_{j=1}^{r}f_j \qquad (3\text{–}6)$$

$$f_j=\begin{cases}\log_4(N/4^h)-1 & (0<j\le 2\cdot 4^h \text{ かつ } j\text{が奇数})\\ \log_4(N/4^h) & (0<j\le 2\cdot 4^h \text{ かつ } j\text{が偶数})\\ \log_4(N/4^{h+i}) & (2\cdot 4^{h+i-1}<j\le 4^{h+i})\\ \log_4(N/4^{h+i})-1 & (4^{h+i}<j\le 2\cdot 4^{h+i} \text{ かつ } j\text{が奇数})\\ \log_4(N/4^{h+i}) & (4^{h+i}<j\le 2\cdot 4^{h+i} \text{ かつ } j\text{が偶数})\\ -1 & (2\cdot 4^{\log_4 N-1}<j\le 4^{\log_4 N}=N)\end{cases}$$

【００８９】

ここで iは $0<i<\log_4(N/4^h)$ を満たす整数である。

【００９０】

(1.4) 各方式の性能比較

図８に受信者総数｜Ｎ｜、無効化したい受信者数｜Ｒ｜＝ｒを一定にしたとき、各方式において受信者が保有しておく秘密情報と伝送するヘッダー量の関係を示す。図８に示すように、Ｎ＝2^{30}＝1,073,741、824≒１０億、ｒ＝2^{14}＝16,384とし、各方式で用いる暗号化アルゴリズムの鍵長は全て128bitとした。

【００９１】

横軸が受信者の保有しておく秘密情報量、縦軸が伝送するヘッダー量の上限を表しており、グラフの左下にある方式ほど、伝送又は蓄える情報量が少ないため、この２点に関しては優れた方式といえる。

【００９２】

実際のシステムの運用においては、受信者ｕは自身が保有する秘密情報I_uから、どの復号鍵（The Subset Difference Method、The Layer Division Subset Difference Methodで擬似乱数生成器を使用する場合はラベル情報）を用いて、伝送されたヘッダー情報を復号するのかを決定する必要がある。その方法としては、例えば、全ての復号鍵で全てのヘッダー情報を復号する方法や、復号に使用すべき復号鍵の情報（ヘッダーの暗号化に使用した暗号鍵のインデックス情報）を付与する方法などが考えられる。この場合伝送される情報はさらにインデックス情報分増加することになるが、図８では考慮していない。

【００９３】

The Subset Difference Methodは全部で19点（丸で示す）プロットされているが、これは、変数bをパラメータとしているためである。左の点からｈ＝18、17、・・・、1、0となっており、一番右端の点が２分木を１つのみ用いた方式に相当する。また、差分集合へのラベルの割り当ては、擬似乱数生成器を用いた方式のみを表示している。

【００９４】

New Method と書かれた方式が本発明の実施形態による方法（The Layer Division Subset Difference Method）であり、これは、差分集合へのラベルの割り当てに擬似乱数生成器を用いていない。本発明の実施形態による方法で擬似乱数生成器を用いた方式は、New Method using PRNG と書かれた方式である。

【００９５】

それぞれ複数の点がプロットされているのは、変数ｄをパラメータとしているためで、左からｄ=1、2、・・・のときを表している。ｄ=1のときは擬似乱数生成器を用いたラベルの割り当てを行っても（受信者が保有する秘密情報量削減という意味での）性能は向上しないことがわかる。また、The Subset Difference

Method と同様にbを変数とすることもできるが、ここでは各ｄについて、伝送するヘッダー量が最小となるパラメータの中で、受信者の保有する秘密情報量が最も少なくなるようなbのみを選択して、その場合のみを表示している。図８には表示していないが、d=1、b=0の場合、アルゴリズムがThe Complete Subtree Method と完全に等価になる。d=16、b=14の場合は、The Subset Difference Method のh=14とした場合と等価になる（図８で２つの方式の結果が重なっている点）。The Tree Pattern Division Method については、アルゴリズムに使用する木を２分木のみでなく任意のn分木を用いる。そのため、図８には、左から使用する木を２分木、３分木、４分木、５分木とした場合の結果を表示している。n分木のリーフに受信者を割り当てるため、２分木、４分木を用いる場合を除いて、受信者総数は$2^{30}=4^{15}$=1、073、741、824にならない。よって、３分木、５分木については以下の値を用いた。

【００９６】

・３分木：$N=3^{19}$=1,162,261,467≒１０億

・５分木：$N=5^{13}$=1,220,703,125≒１０億

また、２分木のとき The Complete Subtree Method とアルゴリズムが完全に等価である。

【００９７】

（1.5）実施形態のコンテンツ配信システム

本発明の実施形態によるコンテンツ配信システムの概略構成を図１（ｂ）に示す。このシステムは、情報提供者７が各種の記憶媒体９をユーザに提供する。本実施形態では、記憶媒体９は、例えばＤＶＤ－ＲＯＭなどの光ディスクを含む各種の記録媒体とすることが可能である。ユーザは再生装置８を所持し、当該再生装置８により記録媒体９から情報を再生する。再生装置８は内部に復号鍵４ａを有している。

【００９８】

ここで、情報提供者７は上記の鍵管理方式の３要素における情報送信者に対応し、再生装置８は情報受信者に対応する。即ち、情報提供者７は、映像／音声などのコンテンツ情報を暗号化用鍵情報５を使用して暗号化し、伝送情報６として

記録媒体９に記録する。また、情報提供者７は、無効化の対象となる再生装置８によっては復号できないが、無効化の対象とならない再生装置８によれば復号可能な鍵情報４ｂを記録媒体９に記録する。そして、情報提供者７は記録媒体９を各再生装置８のユーザに提供する。

【００９９】

無効化の対象とならない再生装置８は、自己の有する復号用鍵４ａで鍵情報４ｂを復号して伝送情報６の復号鍵を取得し、これで伝送情報６を復号して映像／音声などの情報を再生することができる。一方、無効化の対象となる再生装置８は、自己の復号用鍵４ａにより記録媒体９内の鍵情報４ｂを復号することができないので、伝送情報６を復号する鍵を得ることができず、伝送情報６を再生することができない。こうして、本システムでは、記録媒体９上に記録された伝送情報６を特定の再生装置８のみにより再生可能とする。

【０１００】

本発明では、上述の階層分割を伴う鍵管理方式（The Layer Division Subset Difference Method）に従って、再生装置８側の復号用鍵４ａ及び記録媒体９に記録される鍵情報４ｂを生成する。具体的には、ある再生装置８に対して、その再生装置を含むような全ての差分集合に割り当てられている復号鍵（または復号鍵を導けるようなラベル）と、当該再生装置が割り当てられたリーフの属する２分木のルートに割り当てられた復号鍵１つを当該再生装置に復号用鍵４ａとして配布すればよい。こうして、記録媒体中９の鍵情報４ｂの情報量の増加を押さえつつ、再生装置８に保持しておく復号用鍵４ａの情報量を大幅に減少させることができる。

【０１０１】

【実施例】

次に、本発明の実施例に係るコンテンツ配信システムについて説明する。なお、このコンテンツ配信システムは、ＤＶＤなどの光ディスクを記録媒体として使用するものであり、ここでは特にＤＶＤ－ＲＯＭを例にとって説明する。このコンテンツ配信システムでは、情報送信者はコンテンツの著作権者、光ディスク製造工場などに相当する。一方、情報受信者はコンテンツの再生機能を有する装置

（再生装置）であり、ハードウェア又はソフトウェアにより構成されている。

【０１０２】

なお、以下の実施例の説明において、Encryption（）は暗号化アルゴリズム、Decryption（）は復号化アルゴリズムを表すものとする。また、Encryption（引数１、引数２）は引数２を暗号鍵として引数１を暗号化した暗号文を表し、Decryption（引数１、引数２）は引数２を復号鍵として引数１を復号したデータを表す。また、記号“｜”は２つのデータの結合を表し、（データＡ）｜（データＢ）のように用いる。

【０１０３】

（2.1）コンテンツ記録装置

まず、コンテンツ記録装置について説明する。図９はコンテンツをディスクに記録するコンテンツ記録装置５０の構成を示すブロック図であり、情報送信者としての前述のディスク製造工場などに設けられるものである。また、コンテンツ記録装置５０の各部の信号Ｓ１～Ｓ７の内容を図１０及び図１１に示している。なお、ここでのコンテンツは、情報送信者から情報受信者へ送信される前述の伝送情報に対応するものである。

【０１０４】

図９において、コンテンツ入力装置５１はコンテンツを入力する装置であり、図１０（ａ）に示すように、コンテンツに対応する信号Ｓ１を出力する。コンテンツとしては、通常、音楽、映像などのマルチメディアデータが代表的であるが、ここでのコンテンツはそれらに限定されるものではなく、文書などのデータも含まれる。また、コンテンツ入力装置５１としては、コンテンツのマスターデータが記録された磁気テープや、ＤＶＤ－Ｒ、ＤＶＤ－ＲＷ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭなどの記録媒体を読み込んで信号Ｓ１を出力する回路や、ＬＡＮ、インターネットなどの通信回線を経由してアクセスし、そのデータをダウンロードして信号Ｓ１を出力する回路などが挙げられる。

【０１０５】

復号鍵入力装置５２はコンテンツ復号用の鍵Ａを入力する装置であり、図１０（ｂ）に示すように、コンテンツ復号鍵Ａである信号Ｓ２を出力する。コンテン

ツ復号鍵Ａは、情報送信者である著作権者、ディスク製造工場又は鍵管理機関により決定される。

【０１０６】

暗号鍵入力装置５３は、コンテンツ暗号鍵Ａを入力する装置であり、図１０（ｃ）に示すように、コンテンツ暗号鍵Ａである信号Ｓ３を出力する。コンテンツ暗号鍵Ａとコンテンツ復号鍵Ａには、次の関係が成立することが要求される。

【０１０７】

Ｐ＝Decryption（Encryption（任意のデータＰ，コンテンツ暗号鍵Ａ），コンテンツ復号鍵Ａ）

コンテンツ暗号化装置５４は、コンテンツ暗号鍵Ａ（信号Ｓ３）を用いてコンテンツ（信号Ｓ１）を暗号化し、暗号化コンテンツである信号Ｓ４を出力する。図１０（ｄ）に示すように、信号Ｓ４＝Encryption（コンテンツ，コンテンツ暗号鍵Ａ）である。

【０１０８】

なお、この例ではコンテンツ暗号鍵Ａを用いてコンテンツを直接暗号化しているが、コンテンツ自体を暗号化する必要は必ずしもない。例えば、コンテンツ自体は他の暗号鍵Ｃで暗号化し、暗号鍵Ｃに対応する復号鍵Ｃを上記のコンテンツ暗号鍵Ａで暗号化して信号Ｓ４として出力してもよい。つまり、ここでいう「コンテンツ暗号鍵を用いてコンテンツを暗号化する」とは、コンテンツの復号化に少なくともコンテンツ復号鍵Ａを必要とするような方法でコンテンツを変換することを意味する。

【０１０９】

暗号鍵入力装置５５は、コンテンツ復号鍵Ａを暗号化するための複数の暗号鍵B_iを入力する装置であり、Ｎ個の暗号鍵B_1、B_2、・・・B_{N-1}、B_Nを、前述の階層分割を伴う鍵管理方式のアルゴリズムに従って選択し、信号Ｓ５を出力する。図１０（ｅ）に示すように、信号Ｓ５＝暗号鍵B_1｜暗号鍵B_2｜・・・｜暗号鍵B_i｜・・・｜暗号鍵B_{N-1}｜暗号鍵B_Nで表される。これら複数の暗号鍵B_iの組み合わせにより、コンテンツを再生することができる再生装置（上述した「無効化の対象とならない受信者」）が一意に決まる。よって、暗号鍵B_iは再生

を許可する権限を持つ機関（鍵管理機関又は情報送信者）が暗号鍵B_iを決定する。

【０１１０】

鍵暗号化装置５６は、信号Ｓ５として得られる暗号鍵B_iを用いて、信号Ｓ２として得られるコンテンツ復号鍵Ａを暗号化し、それにヘッダー情報Header（暗号鍵B_i）を付加して信号Ｓ６として出力する。図１１（ａ）に示すように、

信号Ｓ６　＝

Header（暗号鍵B_1）｜Encryption（コンテンツ復号鍵Ａ，暗号鍵B_1））

｜Header（暗号鍵B_2）｜Encryption（コンテンツ復号鍵Ａ，暗号鍵B_2））

｜・・・

｜Header（暗号鍵B_i）｜Encryption（コンテンツ復号鍵Ａ，暗号鍵B_i）

｜・・・

｜Header（暗号鍵B_{N-1}｜Encryption（コンテンツ復号鍵Ａ，暗号鍵B_{N-1}）

｜Header（暗号鍵B_N）｜Encryption（コンテンツ復号鍵Ａ，暗号鍵B_N）

で表される。なお、以下の説明では簡単のため、

信号Ｓ６＝Header（暗号鍵Ｂ）｜Encryption（コンテンツ復号鍵Ａ，暗号鍵Ｂ）と表す。

【０１１１】

記録信号生成装置５７は、暗号化されたコンテンツと、複数の暗号鍵B_iで暗号化されたコンテンツ復号鍵Ａの組み合わせとを合成して記録信号を生成する。より具体的には、記録信号生成装置５７は、信号Ｓ４＝Encryption（コンテンツ，コンテンツ暗号鍵Ａ）と、信号Ｓ６＝Header（暗号鍵Ｂ）｜Encryption（コンテンツ復号鍵Ａ，暗号鍵Ｂ）を結合し、それにエラー訂正符号を付加したものを信号Ｓ７として出力する。よって、図１１（ｂ）に示すように、信号Ｓ７は、コンテンツ暗号鍵Ａで暗号化したコンテンツ、Ｎ個の暗号鍵Ｂｉで暗号化されたコンテンツ復号鍵Ａ及びヘッダーにエラー訂正符号を追加した信号であり、

Ｓ７　＝Header（暗号鍵Ｂ）｜Encryption（コンテンツ復号鍵Ａ，暗号鍵Ｂ）

｜Encryption（コンテンツ，コンテンツ暗号鍵Ａ）｜ＥＣＣ

で示される。なお、ＥＣＣはエラー訂正符号である。

【０１１２】

記録装置５８は、生成された記録信号Ｓ７を光ディスクＤに記録し、又は、光ディスクを製造するためのマスターディスクなどに記録信号Ｓ７をカッティングする）に記録する装置であり、通常レーザ光源やレーザ発信器などを備える。

【０１１３】

（2.2）コンテンツ再生装置

次に、上述のようにしてコンテンツが記録された光ディスクＤからコンテンツを再生するためのコンテンツ再生装置６０について説明する。図１２はコンテンツ再生装置６０の構成を示すブロック図である。また、コンテンツ再生装置６０の各部の信号の内容を図１３及び図１４に示している。

【０１１４】

図１２において、情報読取装置６１は光ピックアップなどの装置であり、光ディスクＤに記録されている情報を読み取って信号Ｓ１１を出力する。信号Ｓ１１は、図１３（ａ）に示すように、

Ｓ１１　＝Header（暗号鍵Ｂ）｜Encryption（コンテンツ復号鍵Ａ，暗号鍵Ｂ）｜Encryption（コンテンツ，コンテンツ暗号鍵Ａ）｜ＥＣＣ

で表される。

【０１１５】

エラー訂正装置６２は、入力された信号Ｓ１１のエラー訂正を行う装置であり、信号Ｓ１１中のＥＣＣに基づいてエラー訂正処理を実行する。そして、エラー訂正後の信号を信号Ｓ１２と信号Ｓ１３に分けてそれぞれ鍵復号装置６４及びコンテンツ復号装置６５へ供給する。信号Ｓ１２は暗号鍵B_iで暗号化されたコンテンツ復号鍵Ａのデータであり、Ｓ１２＝Header（暗号鍵Ｂ）｜Encryption（コンテンツ復号鍵Ａ，暗号鍵Ｂ）で示される。一方、信号Ｓ１３はコンテンツ暗号鍵Ａで暗号化されたコンテンツのデータであり、Ｓ１３＝Encryption（コンテンツ，コンテンツ暗号鍵Ａ）で示される。

【０１１６】

記憶装置６３は、再生装置が保有する複数の復号鍵B_1、B_2、・・・、B_j、B_{M-1}、B_MとそのヘッダHeader（B_1）、Header（B_2）、・・・、Header（B_j

）、・・・、Header（B_{M-1}）、Header（B_M）を保存しておく装置である。なお、ここでは記憶装置６３はM個の復号鍵を保有していると仮定する。また、鍵管理機関は、コンテンツ復号鍵Ａの暗号化用の暗号鍵B_iと再生を許可されている再生装置の保有する復号鍵B_jのうちの少なくとも１つは次の関係が整理するように、予め再生装置に復号鍵B_jを配布している：

Ｐ　＝　Decryption（Encryption（任意のデータＰ，暗号鍵Ｂi），復号鍵Ｂj）

さらに、ヘッダーについては、上記の関係の暗号鍵B_iと復号鍵B_jに付加されたヘッダーについて次の関係が成立するようにヘッダーの値が決定されている：

Header（暗号鍵B_i）＝Header（暗号鍵B_j）

上記の関係が成立するように復号鍵B_jとそのヘッダーを各再生装置に（再生装置製造時に）配布するのは、上述の鍵管理機関であり、その際にどの再生装置にどの復号鍵B_jを配布するかの決定は、上述の階層分割を伴う鍵管理方式のアルゴリズムに従って行われる。なお、上述のアルゴリズム中の差分集合への鍵の割り当てにおいて、疑似乱数生成器が用いられる場合は、コンテンツ再生装置６０の記憶装置６３に保有されるのは復号鍵B_jそのものではなく、復号鍵を計算するのに必要なラベル情報である。

【０１１７】

記憶装置６３は、図１４（ｂ）に示すように、復号鍵B_1｜復号鍵B_2｜・・・｜復号鍵B_{M-1}｜復号鍵B_Mと、そのヘッダーHeader（復号鍵B_1）｜Header（復号鍵B_2）｜・・・｜Header（復号鍵B_{M-1}）｜Header（復号鍵B_M）を出力する。

【０１１８】

鍵復号装置６４は、信号Ｓ１２＝Header（復号鍵Ｂ｜Encryption（コンテンツ復号鍵Ａ，暗号鍵Ｂ）と、信号Ｓ１４＝（復号鍵B_1｜復号鍵B_2｜・・・｜復号鍵B_{M-1}｜復号鍵B_M）とそのヘッダーHeader（復号鍵B_1）｜Header（復号鍵B_2）｜・・・｜Header（復号鍵B_j）｜・・・｜Header（復号鍵B_{M-1}）｜Header（復号鍵B_M）を入力とし、光ディスクＤから読み取ったHeader（暗号鍵B_i）と再生装置が保有するHeader（復号鍵B_j）が一致するかを調べ、一致する時には復

号鍵B_jを用いてEncryption（コンテンツ復号鍵Ａ，暗号鍵B_i）を復号する。つまり、コンテンツ復号鍵Ａ＝Decryption（Encryption（コンテンツ復号鍵Ａ，暗号鍵B_i），復号鍵B_j）となる。この処理を一致するヘッダーの組み合わせが見つかるようにｉ及びｊの組み合わせを変えて実行し、図１４（ｃ）に示すように信号Ｓ１５＝コンテンツ復号鍵Ａを出力する。一方、一致するヘッダーの組み合わせがない場合は、再生不可能として全ての処理を終了する。

【０１１９】

なお、前述のように記憶装置６３に復号鍵B_jそのものではなく、復号鍵を計算するのに必要なラベル情報が保存されている場合は、鍵復号装置６４がラベル情報から復号鍵を計算した上で同様の処理を行えばよい。こうして、復号されたコンテンツ復号鍵Ａが信号Ｓ１５としてコンテンツ復号装置６５へ供給される。

【０１２０】

コンテンツ復号装置６５は、図１４（ａ）に示す信号Ｓ１３＝Encryption（コンテンツ，コンテンツ暗号鍵Ａ）と、図１４（ｃ）に示す信号Ｓ１５＝Decryption（Encryption（コンテンツ復号鍵Ａ，暗号鍵B_i），復号鍵B_j）＝コンテンツ復号鍵Ａを入力とし、信号Ｓ１５を用いて信号Ｓ１３を復号し、その結果、Decryption（Encryption（コンテンツ，コンテンツ暗号鍵Ａ），コンテンツ復号鍵Ａ）＝コンテンツを信号Ｓ１６として出力する。再生装置６６はコンテンツ復号装置６５により復号されたコンテンツを再生する。こうして、再生を許可された再生装置のみによりコンテンツの再生が行われる。

【０１２１】

(2.3) コンテンツ記録処理

次に、光ディスクＤへのコンテンツ記録処理について図１５を参照して説明する。図１５はコンテンツ記録処理のフローチャートである。まず、複数存在する再生装置の中で、対象となる光ディスクＤの再生を許可する１つ以上の再生装置を選択する（ステップＳ１）。この処理は、通常は鍵管理機関により行われるが、著作権者、ディスク製造工場などの情報送信者が行う場合もある。

【０１２２】

次に、ステップＳ１で選ばれた、再生を許可する再生装置全てについて、少な

くとも１つは復号鍵が存在し、かつ、再生を許可されていない装置については１つも復号鍵が存在しないような復号鍵の集合のうち最小となる集合を選択する（ステップＳ２）。

【０１２３】

次に、コンテンツ復号鍵Ａを決定し、ステップＳ２で選択された復号鍵の集合に属する全ての復号鍵B_jを、Ｐ＝Decryption（Encryption（任意のデータＰ，暗号鍵B_i），復号鍵B_j）を満たす暗号鍵B_iを用いて暗号化し、Encryption（コンテンツ復号鍵Ａ，暗号鍵B_i）を求める（ステップＳ３）。通常、この処理も鍵管理機関で行われるが、情報送信者が行う場合もある。

【０１２４】

次に、ステップＳ３で選択されたコンテンツ暗号鍵Ａを用いてコンテンツを暗号化し、Encryption（コンテンツ，コンテンツ暗号鍵Ａ）を求める（ステップＳ４）。この処理は、通常、情報送信者が行う。

【０１２５】

次に、ステップＳ３及びＳ４で求められたEncryption（コンテンツ復号鍵Ａ，暗号鍵B_i）及びEncryption（コンテンツ，コンテンツ暗号鍵Ａ）に対してエラー訂正符号を付加する（ステップＳ５）。この処理は、情報送信者である著作権者、ディスク製造工場などで行われる。

【０１２６】

そして、ステップＳ３、Ｓ４及びＳ５で計算されたEncryption（コンテンツ復号鍵Ａ，暗号鍵B_i）及びEncryption（コンテンツ，コンテンツ暗号鍵Ａ）並びにエラー訂正符号を光ディスクＤに記録する（ステップＳ６）。この処理はディスク製造工場など、情報送信者により行われる。こうして、暗号化されたコンテンツ及びその復号鍵の情報が光ディスクＤに記録される。

【０１２７】

次に、上記ステップＳ２における復号鍵の集合の選択処理について図１６を参照して説明する。図１６は、図１５におけるステップＳ２の処理、即ち、再生を許可しない再生装置が与えられたとき、対象ディスクの再生を許可された再生装置の全てについて１つの復号（暗号）鍵が存在し、かつ、再生を許可されていな

い装置については１つも復号（暗号）鍵が存在しないような復号（暗号）鍵の集合のうち、最小となる集合を選択する処理を詳細に示すフローチャートである。

【０１２８】

まず、複数の再生装置をそれぞれリーフに割り当てた2^b個の２分木から、無効化したい（再生を許可しない）再生装置の存在しない２分木について、そのルートに割り当てられた暗号鍵を暗号鍵B_iとして選択する（ステップＳ２１）。このとき、無効化したい再生装置の存在しない２分木は除去し、その後の処理の対象から除外する。

【０１２９】

次に、２分木が存在するか否かを判定する（ステップＳ２２）。存在する場合、無効化したい再生装置又は無効化したい再生装置を含む再生装置の集合の割り当てられているリーフ（この２種類のリーフをまとめて「無効化リーフ」と呼ぶ。）を含む任意の部分木T_hを１つ選び、$ST_h(\underline{R})$を構成する（ステップＳ２３）。ここで、$ST_h(\underline{R})$とは、部分木T_hのルートと無効化リーフを結ぶ最短パス上のノードのみで構成される部分木のことである。また、ここで選択される部分木T_hはどの２分木中に含まれていても構わない。つまり、ステップＳ２１で除去されなかった全ての２分木が対象となっている。

【０１３０】

次に、$ST_h(\underline{R})$中の１つの無効化リーフv_i、v_jを、それらの共通ノードｖ以下に他の無効化リーフが存在しないように選択する（ステップＳ２４）。ここで共通ノードとは、２つの無効化リーフからルートへのパスの共通部分に存在するノードの中で無効化リーフとの距離が最小となるノードのことである。ｖの２つの子ノードの中で、ｖとv_iのパス上に存在する子ノードをv_k、ｖとv_iのパス上に存在する子ノードをv_lとする。（無効化リーフが$ST_h(\underline{R})$中に１つしか存在しない場合、$v_i=v_j$、$v=v_l=v_k$とし、ｖは$ST_h(\underline{R})$のルートとなっている。

【０１３１】

次に、$v_i \neq v_k$ならば、差分集合$S_{k,i}$に割り当てられた暗号鍵をB_iの１つとして選択する（ステップＳ２５）。同様に、$v_l \neq v_j$の場合も差分集合$S_{l,j}$に

割り当てられた暗号鍵をB_iの１つとして選択する。差分集合への鍵の割り当てに疑似乱数生成器を用いている場合は、集合S_k、S_lに割り当てられたラベルから、前述の方法により差分集合$S_{k,i}$、$S_{l,j}$に割り当てられている暗号鍵を計算し、暗号鍵をB_iの１つとして選択する。

【０１３２】

次に、ノードｖより下に位置する部分木T_h中のノードを全て除去し、ｖを無効化リーフとする（ステップＳ２６）。次に、ST_h（R）内のルートノードが無効化リーフであるか否かを判定し（ステップＳ２７）。ルートノードが無効化リーフである場合は、ルートノード以外に無効化リーフを含む他の部分木T_hが全ての２分木中に存在するか否かを判定する（ステップＳ２８）。存在する場合、処理はステップＳ２３に戻り、ルートノード以外に無効化リーフを含む他の部分木T_hを選択し、同様の処理を繰り返す。

【０１３３】

一方、ステップＳ２７でST_h（R）内のルートノードが無効化リーフでないと判定された場合、処理はステップＳ２４へ戻り他の無効化リーフを選択して同様の処理を行う。

【０１３４】

こうして、ルートノード以外に無効化リーフを含む他の部分木T_hが全ての２分木中に存在しなくなったとき（ステップＳ２８；No）、処理は終了する。コンテンツ復号鍵Ａの暗号化に用いられる暗号鍵B_iの集合は、ステップＳ２１及びステップＳ２５で選択され（又はラベルから計算）された暗号鍵となる。

【０１３５】

（2.4）コンテンツ再生処理

次に、光ディスクＤからのコンテンツ再生処理について説明する。図１７はコンテンツ再生処理のフローチャートである。まず、光ディスクＤから光ピックアップなどの読取装置６１により記録情報が読み取られる（ステップＳ３１）。次に、ステップＳ３１で得られた信号に対してエラー訂正装置６２によりエラー訂正を行う（ステップＳ３２）。

【０１３６】

次に、光ディスクＤ中に記録されているＮ個のヘッダーHeader（暗号鍵B_i）の中に、再生装置が保有するＭ個の復号鍵B_jのヘッダーHeader（復号鍵B_j）の少なくとも１つは一致するものが存在するか否かを調べる（ステップＳＳ３３）。存在する場合、その再生装置は再生を許可されたものであることになり、一致した光ディスクＤ側のヘッダーHeader（暗号鍵B_i）に対応するEncryption（コンテンツ復号鍵Ａ，暗号鍵B_i）を、再生装置側のヘッダーHeader（復号鍵B_j）に対応する復号鍵B_jで復号する（ステップＳ３４）。つまり、コンテンツ復号鍵Ａ＝Decryption（Encryption（コンテンツ復号鍵Ａ，暗号鍵B_i），復号鍵B_j）という処理を行い、コンテンツ復号鍵Ａを得る。

【０１３７】

次に、ステップＳ３４で復号されたコンテンツ復号鍵Ａを用いて、光ディスクＤ上の暗号化コンテンツであるEncryption（コンテンツ，コンテンツ暗号鍵Ａ）を復号する（ステップＳ３５）。つまり、コンテンツ＝Decryption（Encryption（コンテンツ，コンテンツ暗号鍵Ａ），コンテンツ復号鍵Ａ）という処理を行い、コンテンツの復号を行う。そして、復号されたコンテンツを再生する（ステップＳ３６）。

【０１３８】

なお、ステップＳ３３で一致するヘッダーが見つからない場合は（ステップＳ３３；No）、その再生装置による再生が許可されていないことになり、コンテンツの再生は行われず、処理は終了する。

【０１３９】

(2.5) 差分集合への暗号鍵の割り当てに疑似乱数生成器を使用する場合

次に、本発明による階層分割を伴う鍵管理方式において差分集合へ暗号（復号）鍵を割り当てる際に疑似乱数生成器を用いる場合の処理を図１８のフローチャートを参照して説明する。

【０１４０】

まず、2^b個の各２分木のルートに独立な値をもつ暗号（復号）鍵を割り当てる（ステップＳ４１）。次に、2^b個の２分木中に含まれる全てのノードに独立な値を持つラベルを割り当てる（ステップＳ４２）。但し、１台の再生装置のみ

が割り当てられているノード（リーフ）は除外される。そして、任意の部分木T_hを選択し（ステップＳ４３）、選択された部分木T_h中の任意のノードv_iをルートとする部分木$T_{h,i}$を選択する（ステップＳ４４）。

【０１４１】

次に、ステップＳ４４で選択された部分木$T_{h,i}$のルートノードに割り当てられたラベルLABEL$_i$（ステップＳ４２で割り当てられている）を用いて、差分集合$\underline{S}_{i,*}$に暗号（復号）鍵$L_{i,*}$を割り当てる（ステップＳ４５）。ここで、＊は部分木$T_{h,i}$中の任意のノードv_*を表す。（但し、$T_{h,i}$のルートノードv_iは除く）。各差分集合への暗号（復号）鍵の割り当ては以下のように行う。

【０１４２】

始めに疑似乱数生成器Ｇの入力をラベルLABEL$_{i,*}$としたとき、その出力を３等分した左側部分をG_L（LABEL$_{i,*}$）、中央部分をG_M（LABEL$_{i,*}$）、右側部分をG_R（LABEL$_{i,*}$）で表す。このとき各出力を以下のように定義する。

【０１４３】

G_L（LABEL$_{i,*}$）　入力ラベルLABEL$_{i,*}$の割り当てられたノードの左側の子ノードに割り当てるラベル

G_M（LABEL$_{i,*}$）　入力ラベルLABEL$_{i,*}$の割り当てられたノードに割り当てる暗号鍵$L_{i,*}$（これが差分集合$\underline{S}_{i,*}$に割り当てられる暗号（復号）鍵になる）

G_R（LABEL$_{i,*}$）　入力ラベルLABEL$_{i,*}$の割り当てられたノードの右側の子ノードに割り当てるラベル

部分木$T_{h,i}$のルートノードに割り当てられたラベルLABEL$_i$からその２つの子ノードのラベルを疑似乱数生成器Ｇを用いて割り当てる。この処理を次は子ノードのラベルを入力として行い、孫ノードのラベルを求める。以下、同様にして部分木$T_{h,i}$中の全てのノードにラベルを割り当てることができる。

【０１４４】

最後に、部分木$T_{h,i}$中の各ノードに割り当てられたラベルLABEL$_{i,*}$を入力として$L_{i,*}=G_M$（LABEL$_{i,*}$）を計算する。この値が差分集合$\underline{S}_{i,*}$に割り当てられる暗号（復号）鍵である。

【０１４５】

次に、ステップＳ４３で選択された部分木T_h中の部分木$T_{h,i}$で、ステップＳ４４で選択されていない部分木が存在するか否かを判定する（ステップＳ４６）。存在する場合はステップＳ４４へ戻り、未だ選択されていない部分木$T_{h,i}$を選択し、同様の処理を行う。存在しない場合は、次に、2^b個の２分木中に存在する全ての部分木T_hの中で、ステップＳ４３で選択されていない部分木T_hが存在するか否かを判定する（ステップＳ４７）。存在する場合は、ステップＳ４３に戻り、まだ選択されていない部分木T_hを選択し、同様の処理を行う。一方、存在しない場合は処理を終了する。

【０１４６】

以上述べたように、本実施例においては、２分木を複数のレイヤに分割し、分割された各部分木に対してThe Subset Difference Methodを適用するので、記録媒体中の鍵情報量の増加を押さえつつ、再生装置の保有しておく復号鍵などの秘密情報を大幅に減少させることができる。

【０１４７】

また、The Subset Difference Methodにおいて、各差分集合への復号（暗号）鍵の割り当てに疑似乱数生成器を用いる場合、再生装置側で保有しているラベル情報から復号鍵を求めるのに最大$\log_2$（Ｎ）＋１回の（疑似乱数生成器の出力を求めるという）演算を必要としていたが、本方式では最大ｄ＋１回で十分となる。なお、ｄは部分木T_hの高さである。よって、ラベル情報から復号鍵を効率的かつ迅速に得ることが可能となる。

【図面の簡単な説明】

【図１】

木構造を用いた鍵管理方式のモデルを示す図である。

【図２】

鍵管理方式により用いる木構造の例を示す図である。

【図３】

鍵管理方式により用いる木構造の例を示す図である。

【図４】

階層分割を伴う鍵管理方式の木構造の例を示す図である。

【図５】

階層分割を伴う鍵管理方式の木構造の例を示す図である。

【図６】

階層分割を伴う鍵管理方式の木構造の例を示す図である。

【図７】

階層分割を伴う鍵管理方式の木構造の例を示す図である。

【図８】

複数の鍵管理方式における記憶媒体側と受信機側の鍵情報サイズを比較するグラフである。

【図９】

本発明の実施例に係るコンテンツ記録システムの構成を示すブロック図である。

【図１０】

図９に示すコンテンツ記録システムの各部の信号内容を示す。

【図１１】

図９に示すコンテンツ記録システムの各部の信号内容を示す。

【図１２】

本発明の実施例に係るコンテンツ再生システムの構成を示すブロック図である。

【図１３】

図１２に示すコンテンツ再生システムの各部の信号内容を示す。

【図１４】

図１２に示すコンテンツ再生システムの各部の信号内容を示す。

【図１５】

コンテンツ記録処理のフローチャートである。

【図１６】

コンテンツ記録処理における復号鍵の選択処理のフローチャートである。

【図１７】

コンテンツ再生処理のフローチャートである。

【図１８】

本発明の鍵管理方式により部分集合に鍵を割り当てる処理のフローチャートである。

【符号の説明】

１　鍵管理機関

２　情報送信者

３　情報受信者

４ａ　復号用鍵

４ｂ　鍵情報

５　暗号化用鍵情報

６　伝送情報

７　情報提供者

８　再生装置

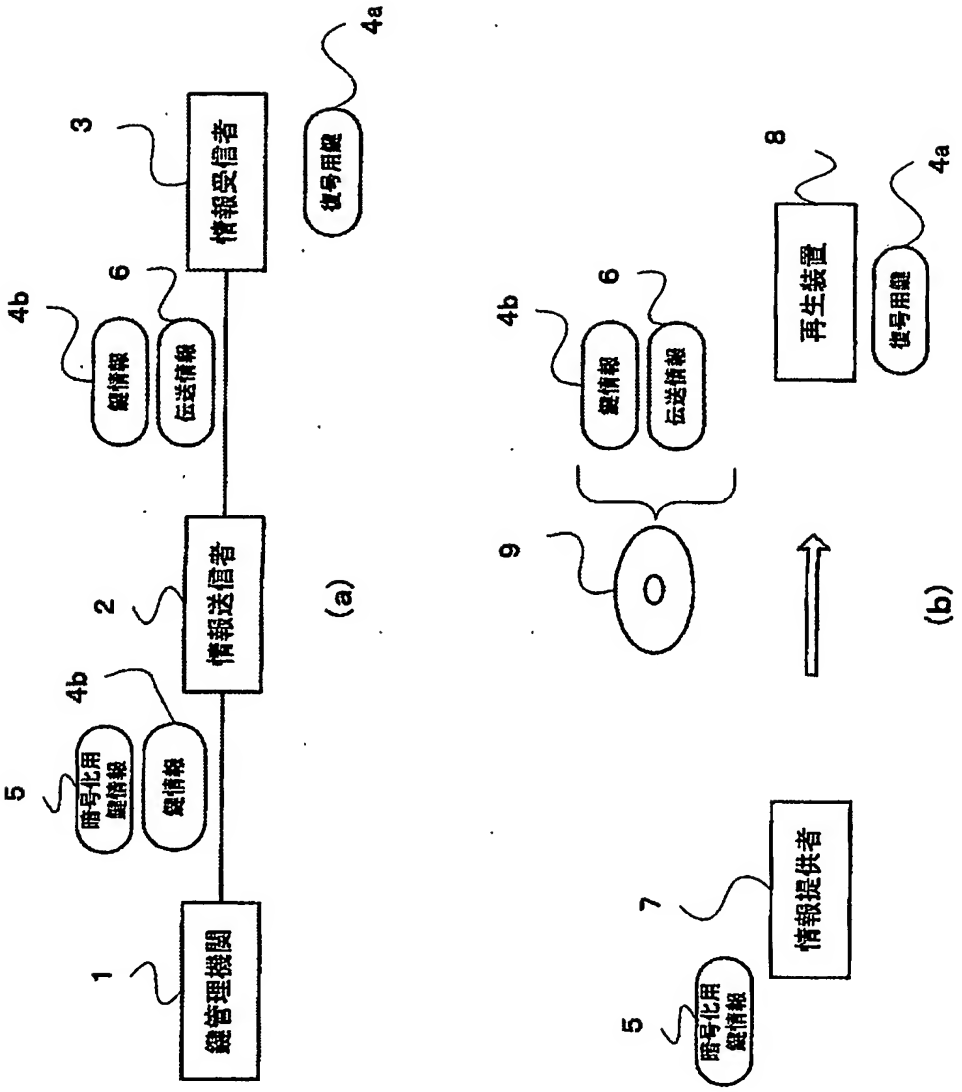
９　記録媒体

５０　コンテンツ記録装置

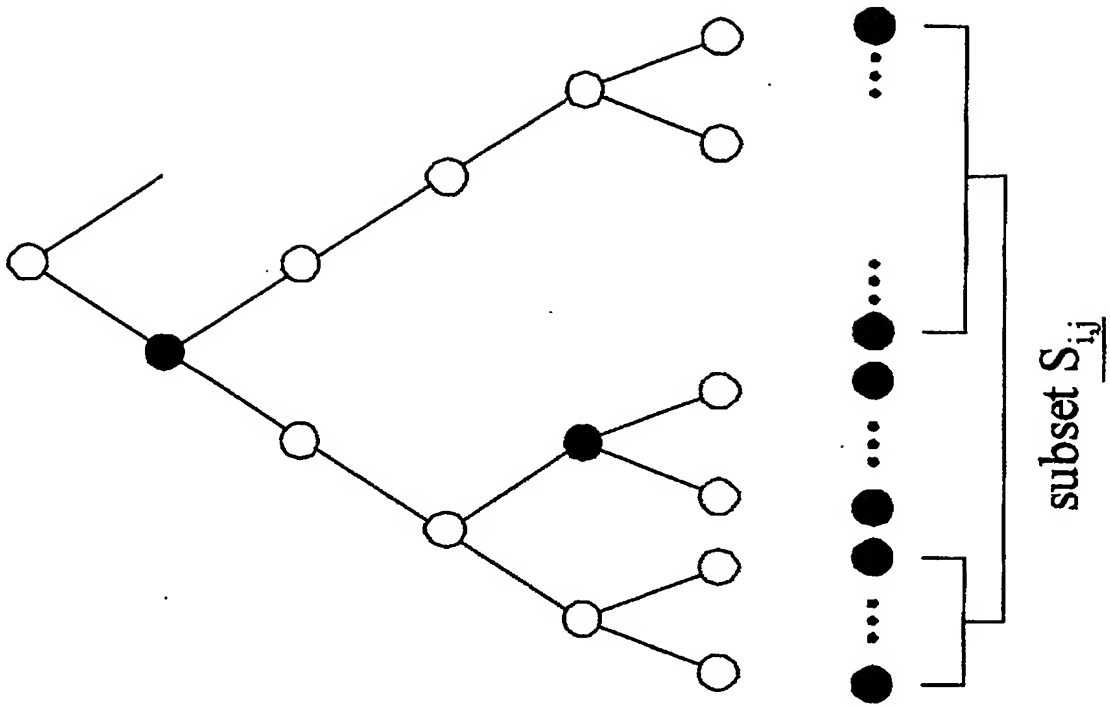
６０　コンテンツ再生装置

【書類名】　　図面

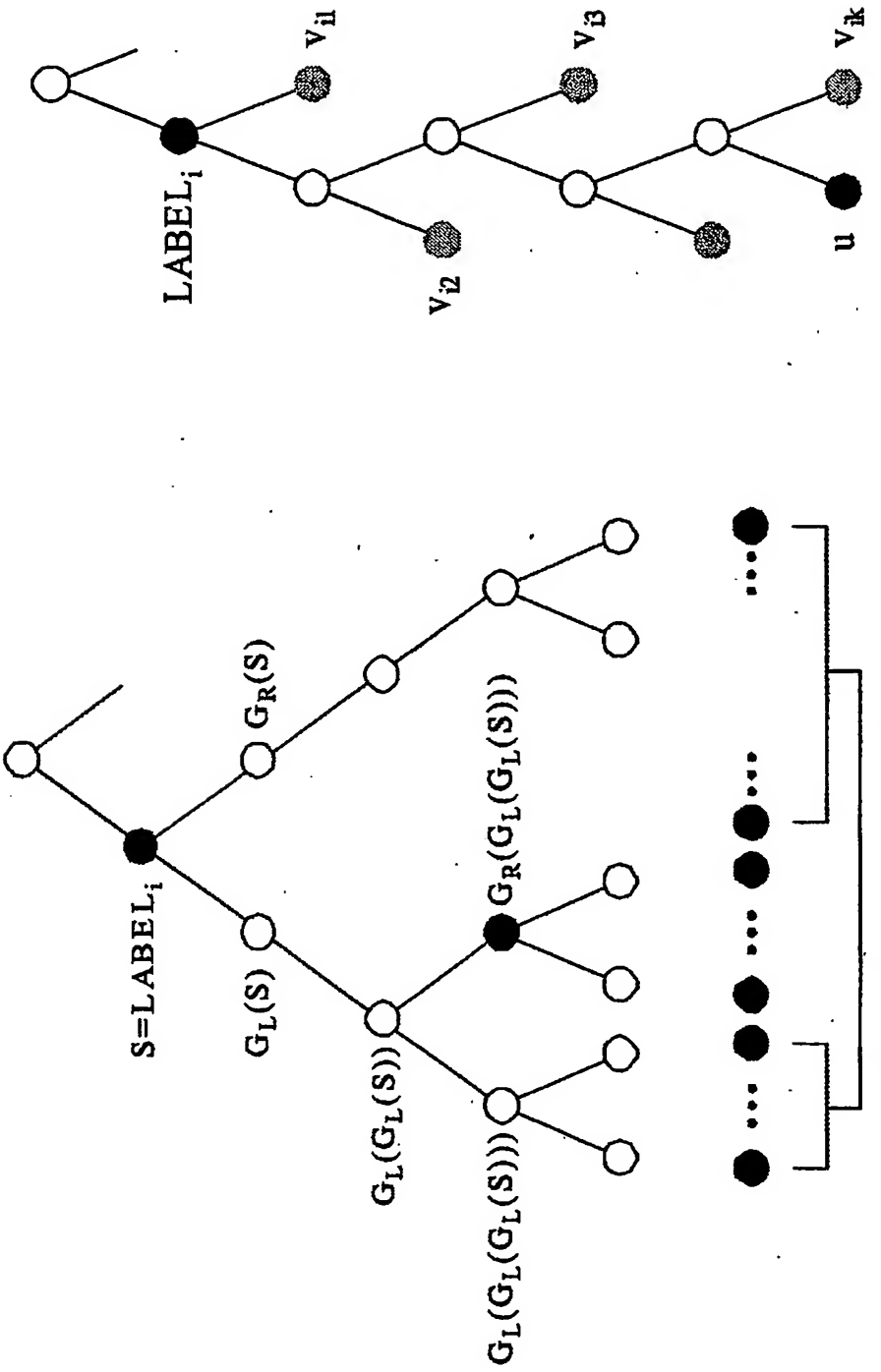
【図１】


鍵管理機関
1
暗号化用鍵情報
5
鍵情報
4b
情報送信者
2
(a)
鍵情報
4b
伝送情報
6
情報受信者
3
復号用鍵
4a
暗号化用鍵情報
5
情報提供者
7
9
鍵情報
4b
伝送情報
6
再生装置
8
復号用鍵
4a
(b)

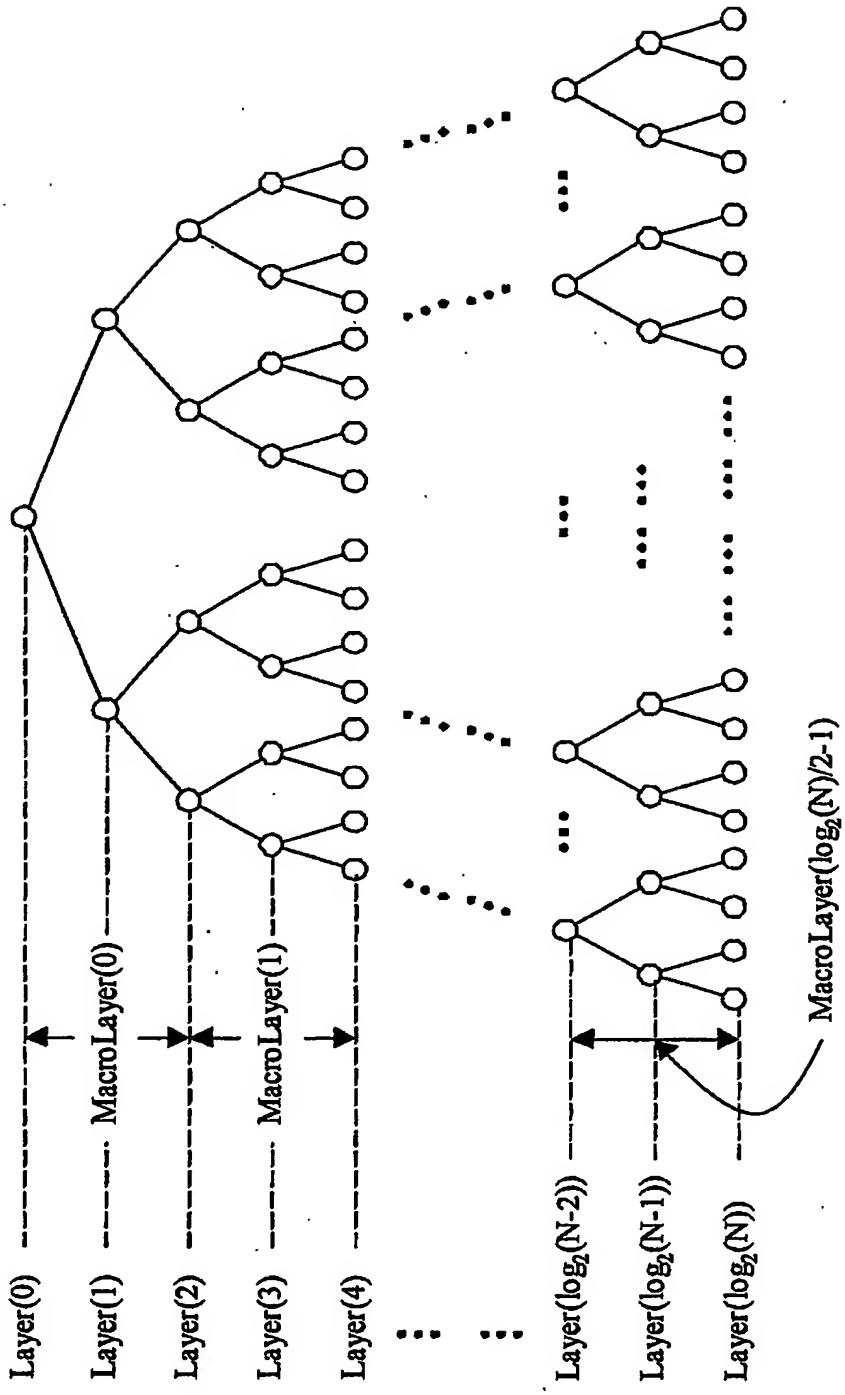
【図２】



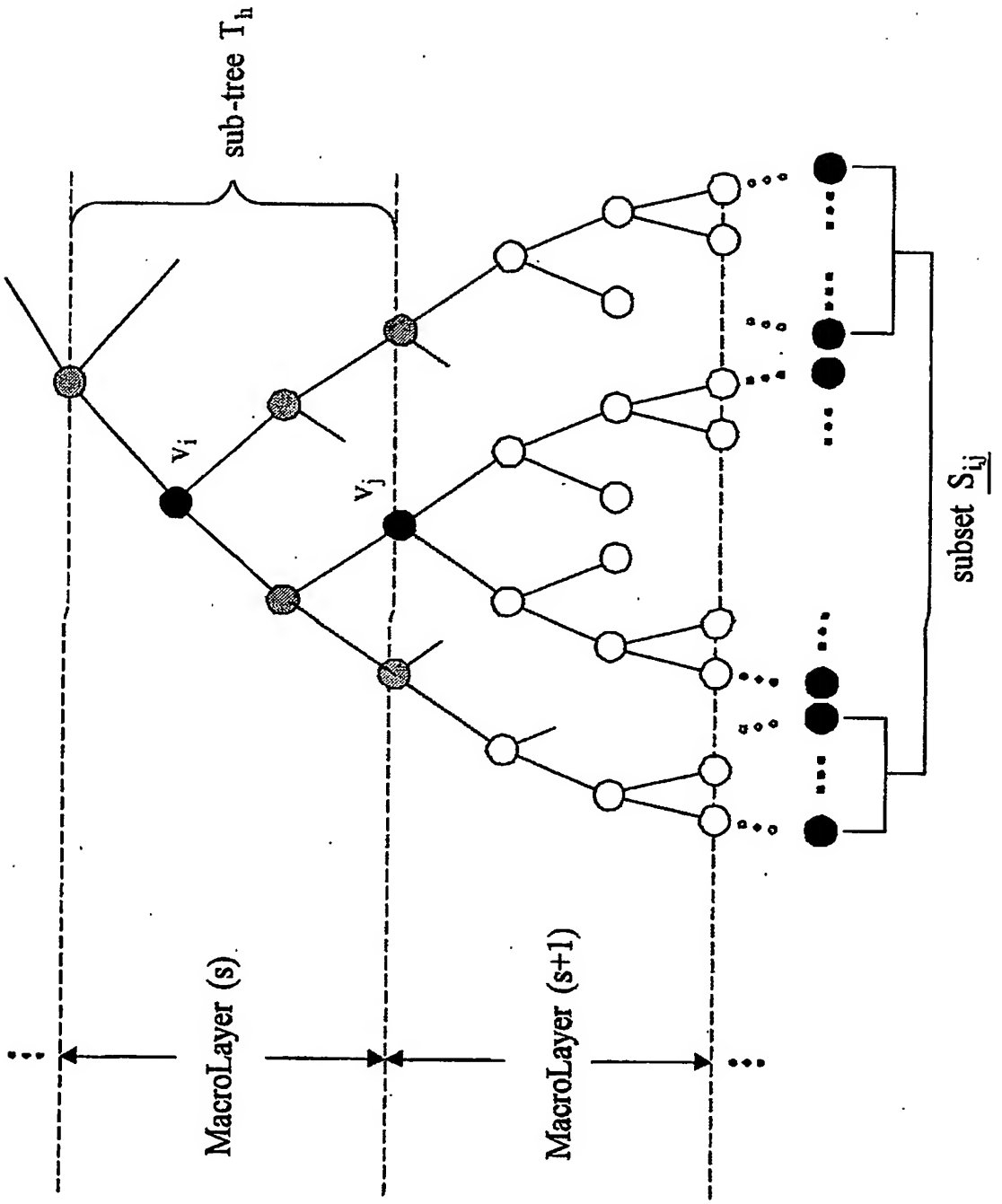
【図３】


S=LABEL$_i$
$G_L(S)$
$G_R(S)$
$G_L(G_L(S))$
$G_R(G_L(G_L(S)))$
$G_L(G_L(G_L(S)))$
(a)
LABEL$_i$
v_{i1}
v_{i2}
v_{i3}
v_{ik}
u
(b)
$L_{i,j}=G_M(LABEL_{i,j})$
$LABEL_{i,j}=G_R(G_L(G_L(LABEL_i)))$

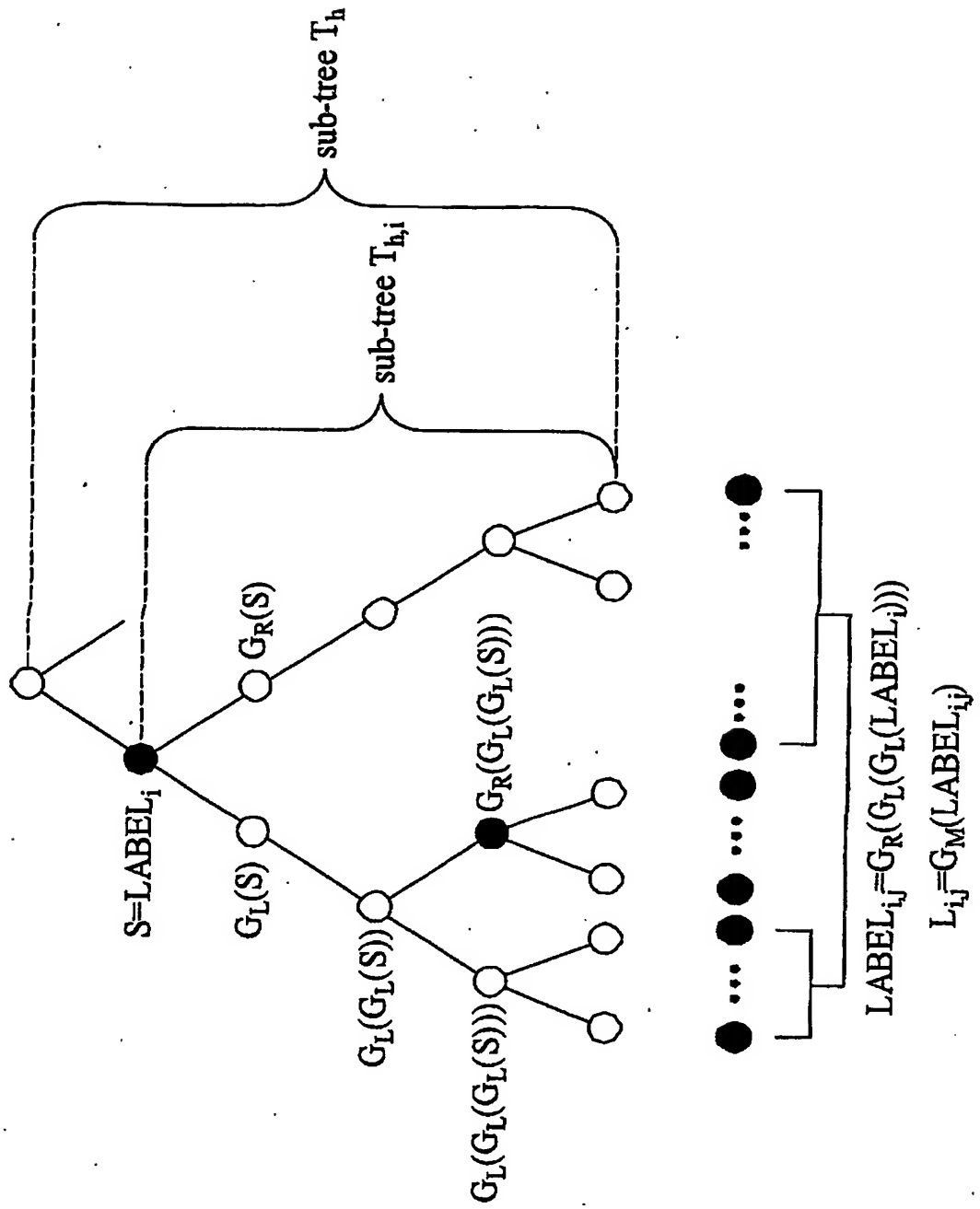
【図４】


Layer(0)
Layer(1)
Layer(2)
Layer(3)
Layer(4)
Layer(log2(N-2))
Layer(log2(N-1))
Layer(log2(N))
MacroLayer(0)
MacroLayer(1)
MacroLayer(log2(N)/2-1)

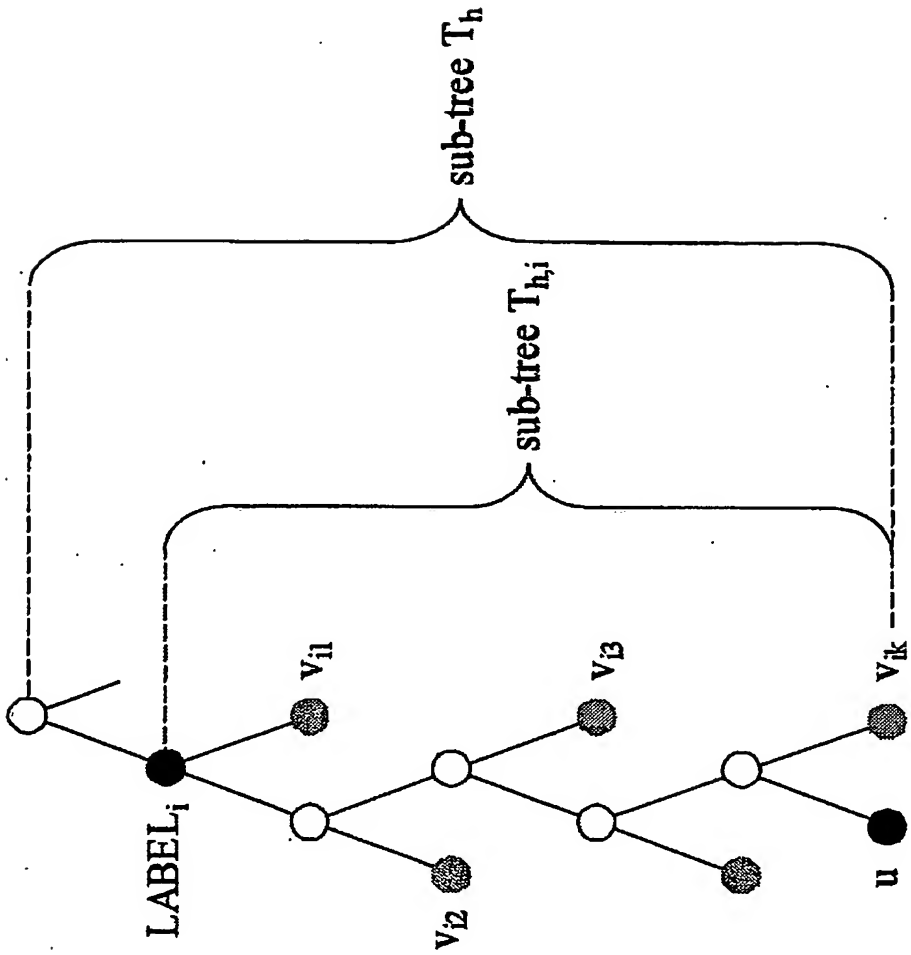
【図５】



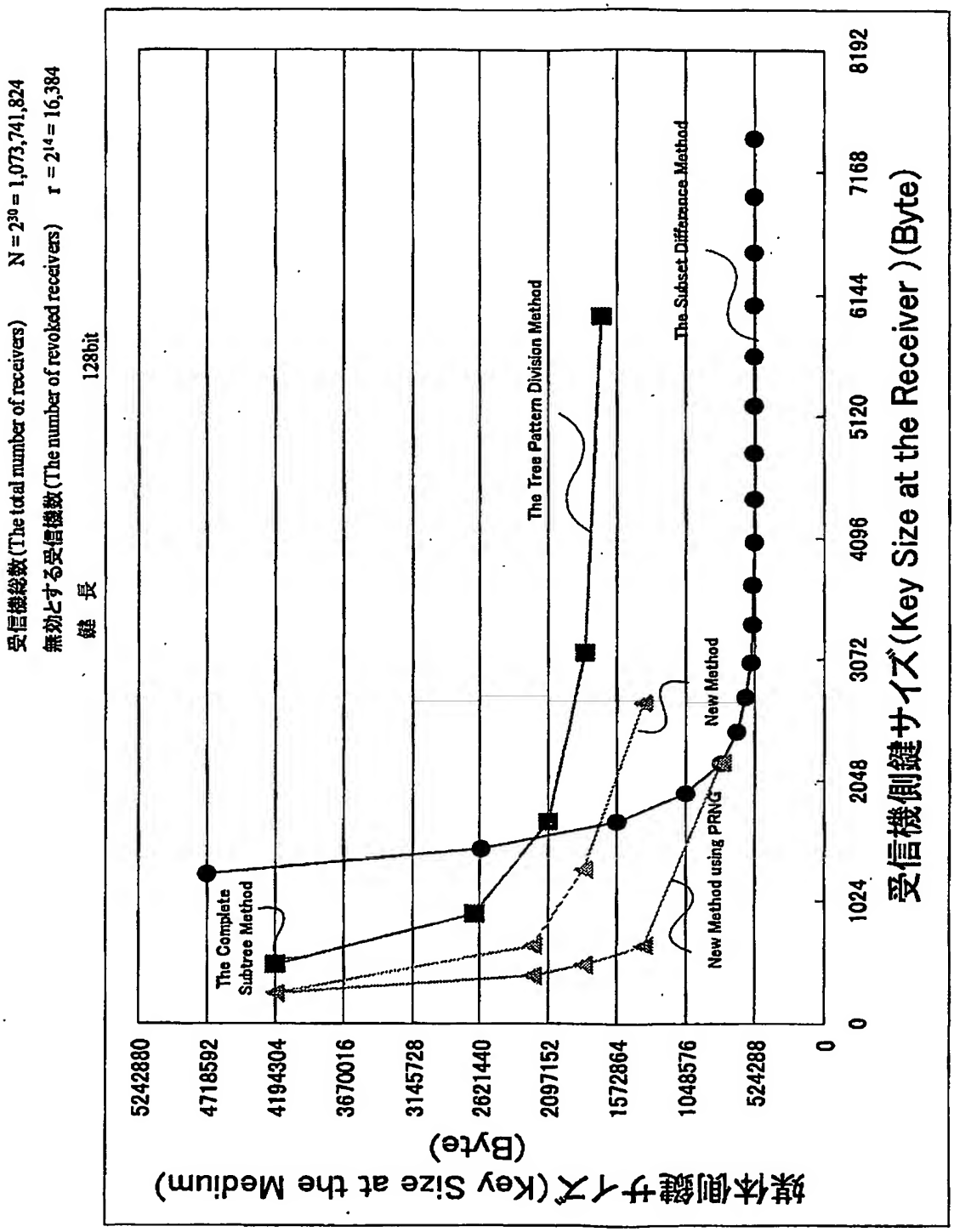
【図６】


sub-tree T_h
sub-tree $T_{h,i}$
$S=LABEL_i$
$G_L(S)$
$G_R(S)$
$G_L(G_L(S))$
$G_R(G_L(G_L(S)))$
$G_L(G_L(G_L(S)))$
$LABEL_{ij}=G_R(G_L(G_L(LABEL_i)))$
$L_{ij}=G_M(LABEL_{ij})$

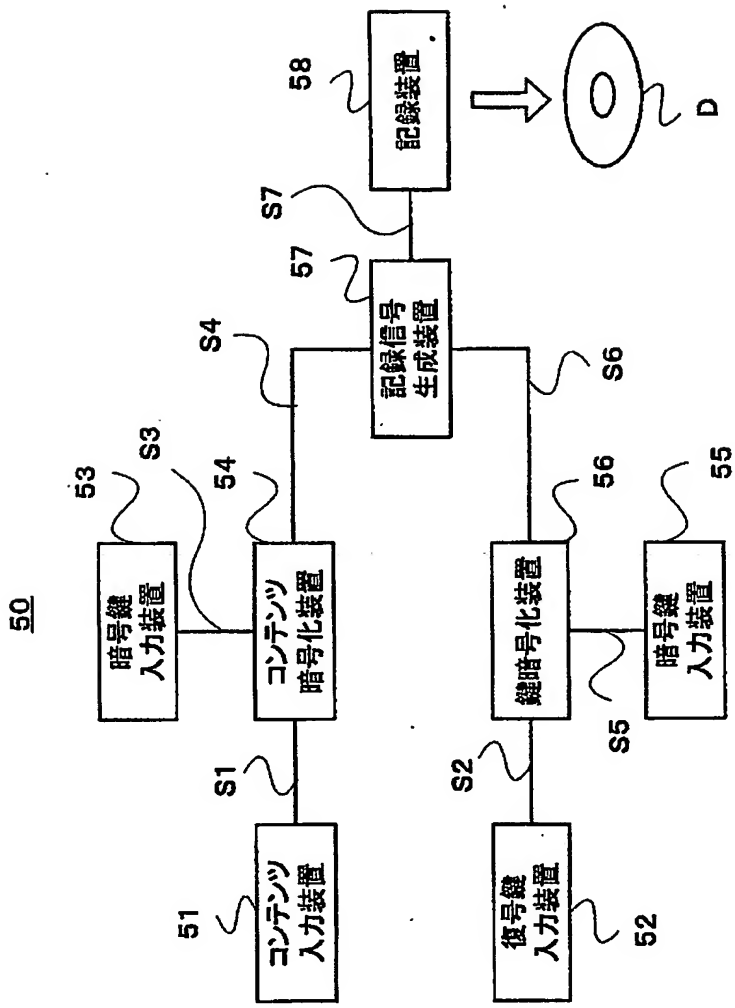
【図７】



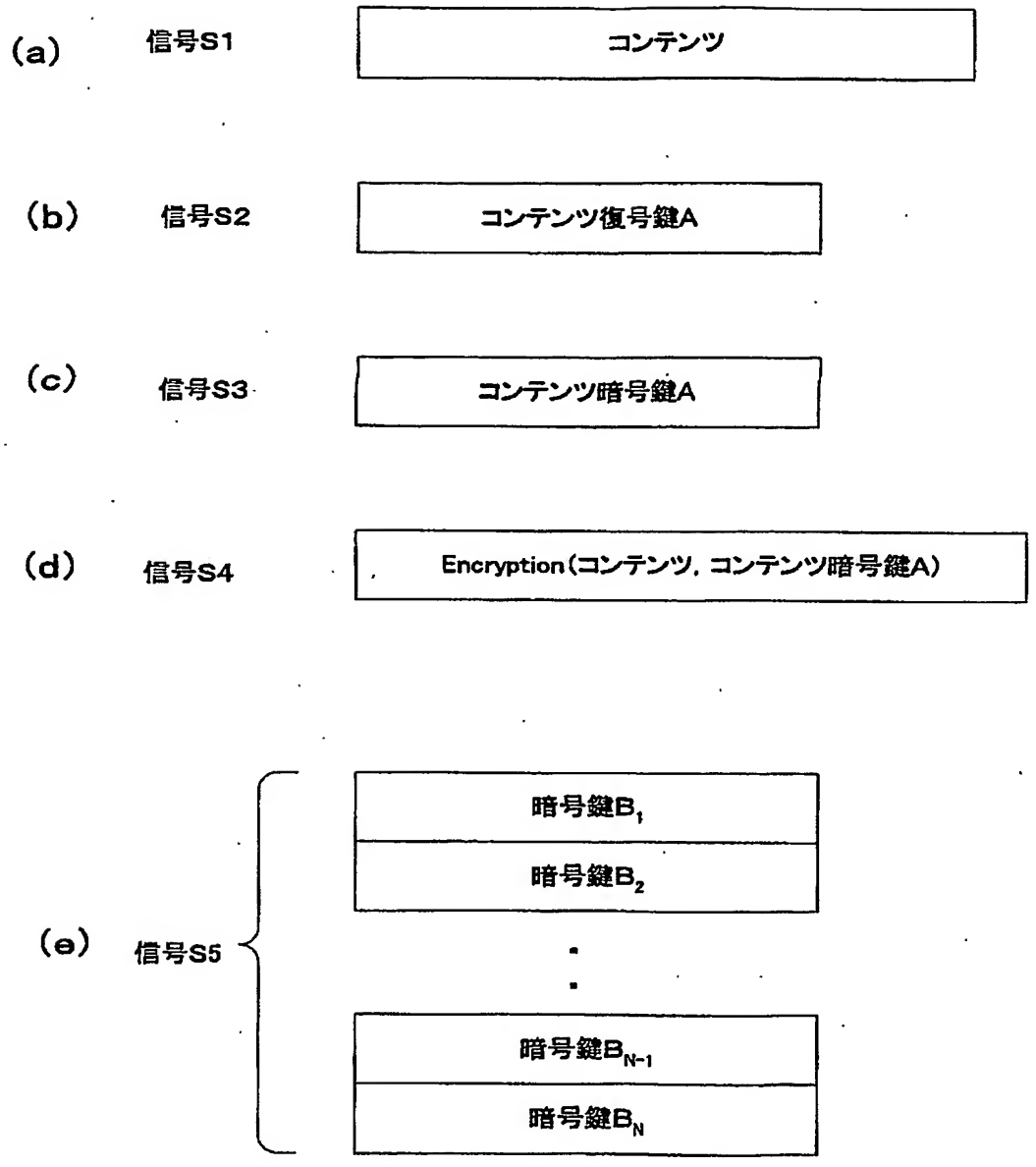
【図８】


受信機総数(The total number of receivers)　N = 2^30 = 1,073,741,824
無効とする受信機数(The number of revoked receivers)　r = 2^14 = 16,384
鍵　長　128bit
媒体側鍵サイズ(Key Size at the Medium) (Byte)
5242880
4718592
4194304
3670016
3145728
2621440
2097152
1572864
1048576
524288
0
The Complete Subtree Method
The Tree Pattern Division Method
The Subset Difference Method
New Method
New Method using PRNG
0
1024
2048
3072
4096
5120
6144
7168
8192
受信機側鍵サイズ(Key Size at the Receiver)(Byte)

【図９】


50
51
コンテンツ入力装置
52
復号鍵入力装置
53
暗号鍵入力装置
54
コンテンツ暗号化装置
55
暗号鍵入力装置
56
鍵暗号化装置
57
記録信号生成装置
58
記録装置
D
S1
S2
S3
S4
S5
S6
S7

【図１０】


(a)
信号S1
コンテンツ
(b)
信号S2
コンテンツ復号鍵A
(c)
信号S3
コンテンツ暗号鍵A
(d)
信号S4
Encryption(コンテンツ, コンテンツ暗号鍵A)
(e)
信号S5
暗号鍵B1
暗号鍵B2
暗号鍵BN-1
暗号鍵BN

【図１１】

信号S6

Header(暗号鍵B_1)	Encryption(コンテンツ復号鍵A, 暗号鍵B_1)
Header(暗号鍵B_2)	Encryption(コンテンツ復号鍵A, 暗号鍵B_2)
⋮	
Header(暗号鍵B_{N-1})	Encryption(コンテンツ復号鍵A, 暗号鍵B_{N-1})
Header(暗号鍵B_N)	Encryption(コンテンツ復号鍵A, 暗号鍵B_N)

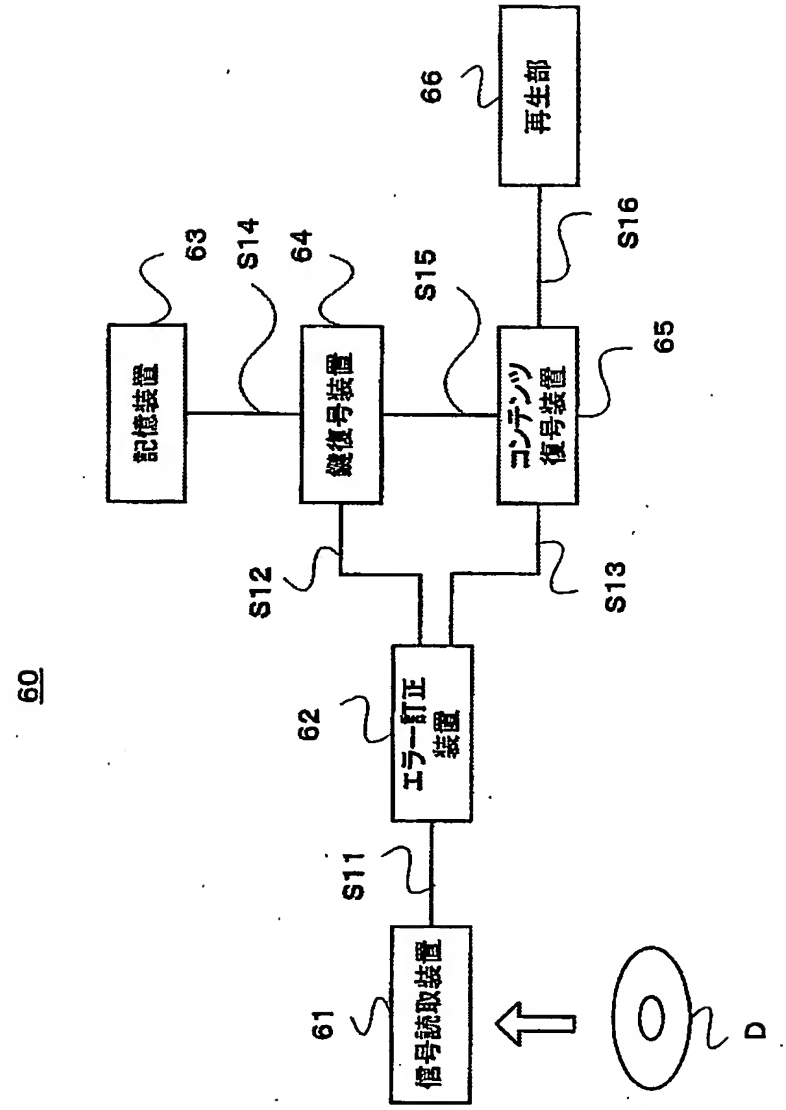
(a)

信号S7

Header(暗号鍵B_1)	Encryption(コンテンツ復号鍵A, 暗号鍵B_1)
Header(暗号鍵B_2)	Encryption(コンテンツ復号鍵A, 暗号鍵B_2)
⋮	
Header(暗号鍵B_{N-1})	Encryption(コンテンツ復号鍵A, 暗号鍵B_{N-1})
Header(暗号鍵B_N)	Encryption(コンテンツ復号鍵A, 暗号鍵B_N)
Encryption(コンテンツ, コンテンツ暗号鍵A)	
Error Correcting Code	

(b)

【図１２】


60
61
信号読取装置
S11
62
エラー訂正装置
S12
S13
63
記憶装置
S14
64
鍵復号装置
S15
65
コンテンツ復号装置
S16
66
再生部
D

【図１３】

信号S11

Header(暗号鍵B_1)	Encryption(コンテンツ復号鍵A, 暗号鍵B_1)
Header(暗号鍵B_2)	Encryption(コンテンツ復号鍵A, 暗号鍵B_2)
・	・
・	・
Header(暗号鍵B_{N-1})	Encryption(コンテンツ復号鍵A, 暗号鍵B_{N-1})
Header(暗号鍵B_N)	Encryption(コンテンツ復号鍵A, 暗号鍵B_N)
Encryption(コンテンツ, コンテンツ暗号鍵A)	
Error Correcting Code	

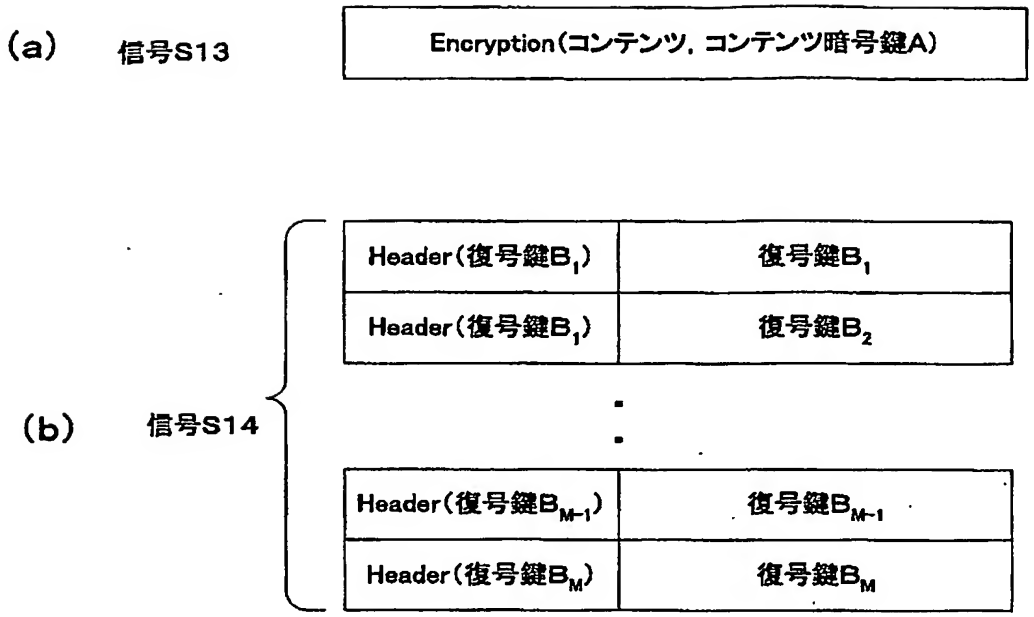
(a)

信号S12

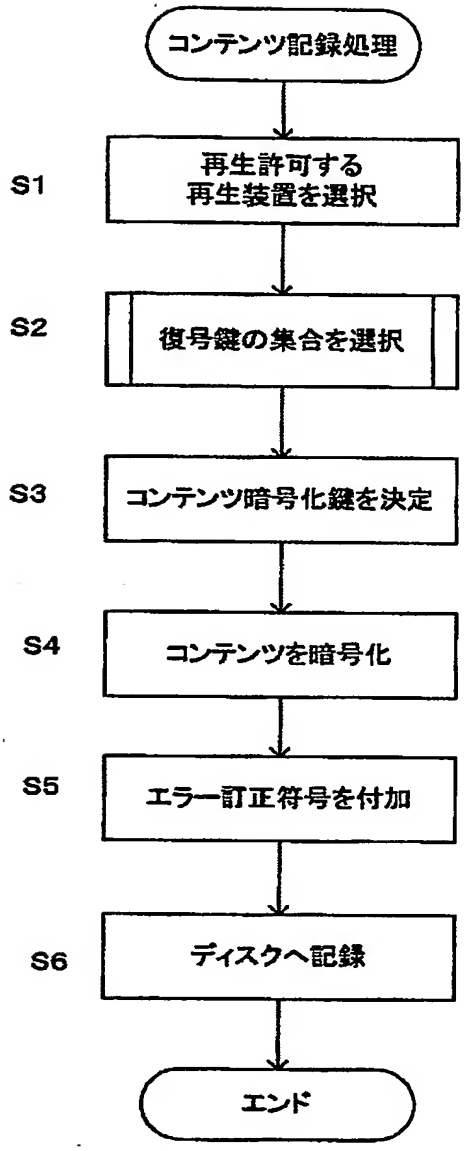
Header(暗号鍵B_1)	Encryption(コンテンツ復号鍵A, 暗号鍵B_1)
Header(暗号鍵B_2)	Encryption(コンテンツ復号鍵A, 暗号鍵B_2)
・	・
・	・
Header(暗号鍵B_{N-1})	Encryption(コンテンツ復号鍵A, 暗号鍵B_{N-1})
Header(暗号鍵B_N)	Encryption(コンテンツ復号鍵A, 暗号鍵B_N)

(b)

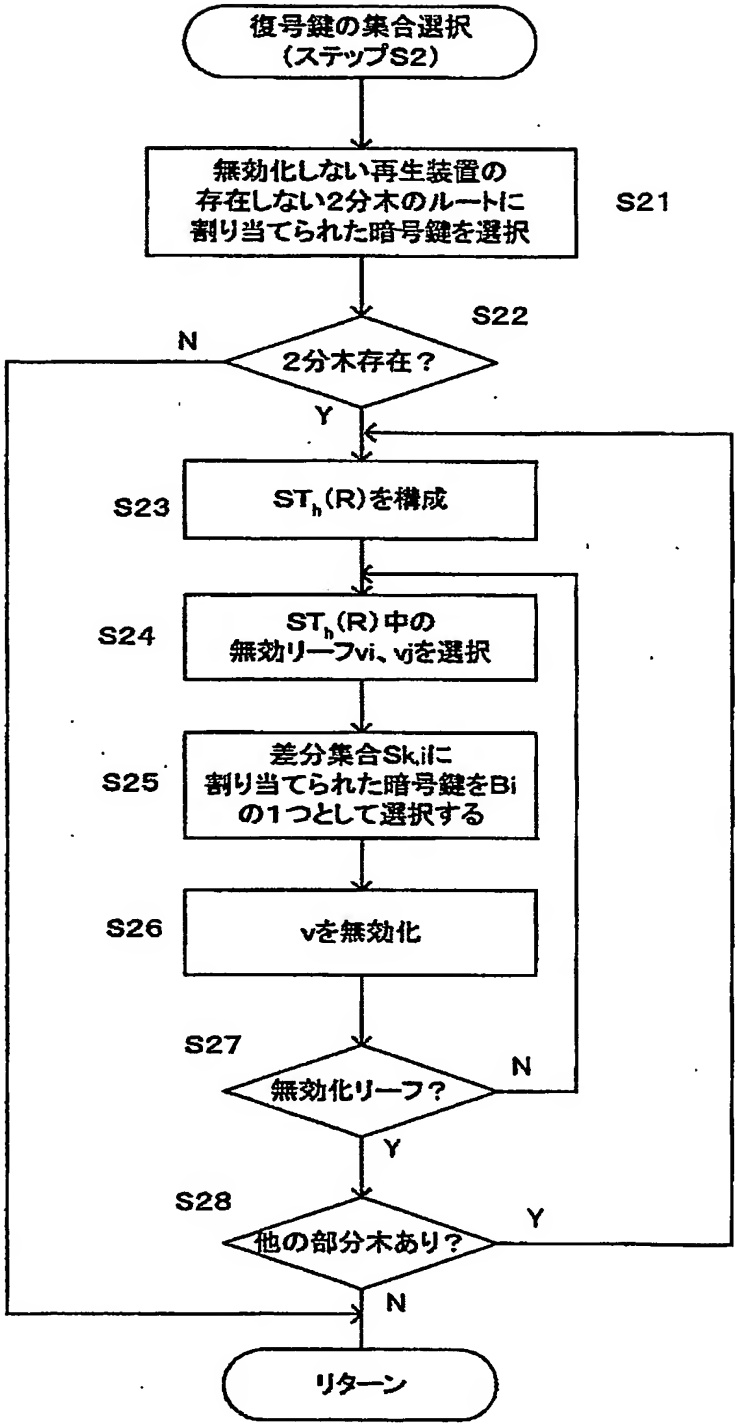
【図１４】


(a)
信号S13
Encryption(コンテンツ, コンテンツ暗号鍵A)
(b)
信号S14
Header(復号鍵B_1)
復号鍵B_1
Header(復号鍵B_1)
復号鍵B_2
Header(復号鍵B_{M-1})
復号鍵B_{M-1}
Header(復号鍵B_M)
復号鍵B_M
(c)
信号S15
コンテンツ復号鍵A
(d)
信号S16
コンテンツ

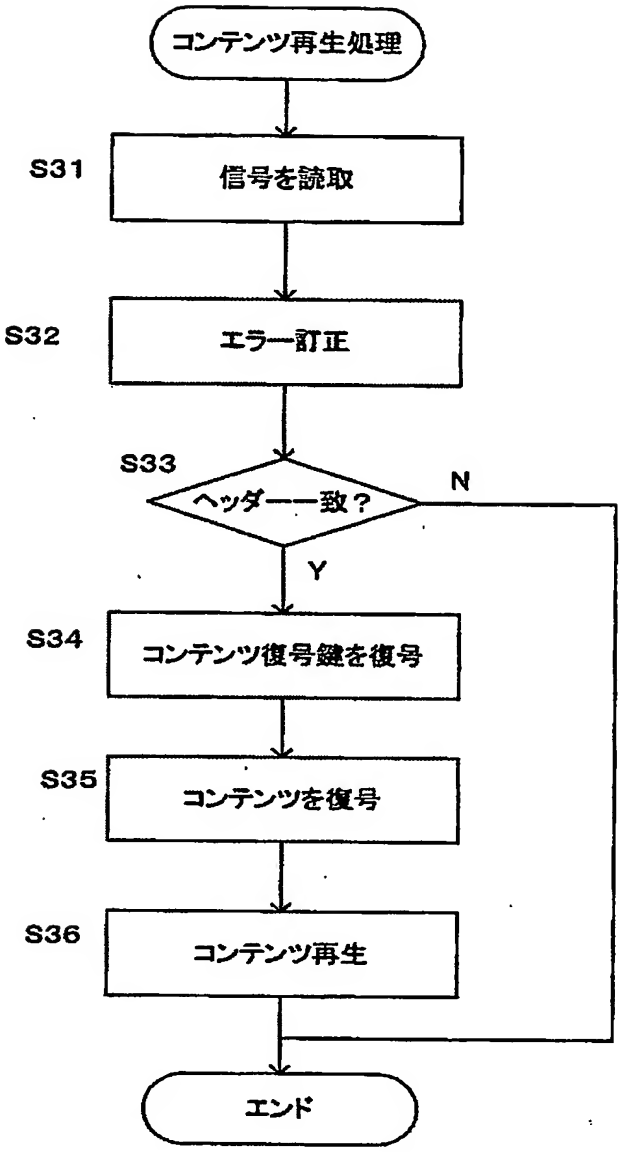
【図１５】


コンテンツ記録処理
S1
再生許可する
再生装置を選択
S2
復号鍵の集合を選択
S3
コンテンツ暗号化鍵を決定
S4
コンテンツを暗号化
S5
エラー訂正符号を付加
S6
ディスクへ記録
エンド

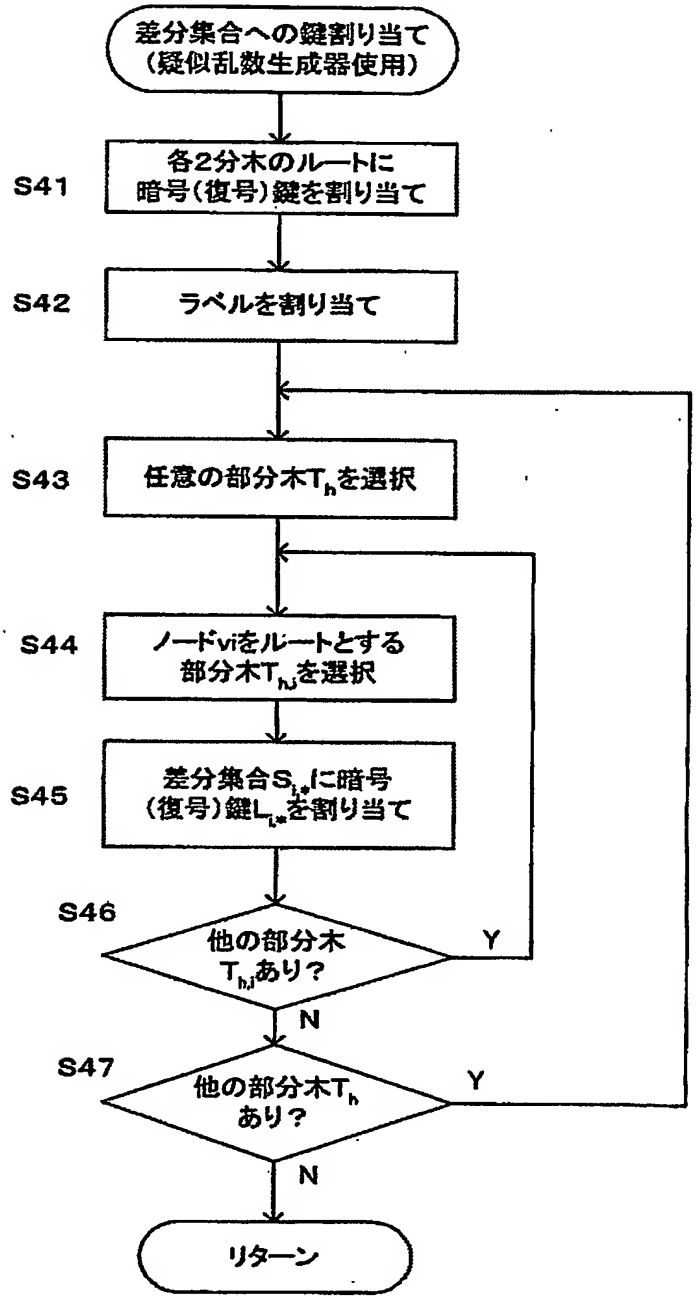
【図１６】


復号鍵の集合選択
（ステップS2）
無効化しない再生装置の
存在しない2分木のルートに
割り当てられた暗号鍵を選択
S21
S22
N
2分木存在？
Y
S23
$ST_h(R)$を構成
S24
$ST_h(R)$中の
無効リーフvi、vjを選択
S25
差分集合Sk,iに
割り当てられた暗号鍵をBi
の1つとして選択する
S26
vを無効化
S27
無効化リーフ？
N
Y
S28
他の部分木あり？
Y
N
リターン

【図１７】


コンテンツ再生処理
S31
信号を読取
S32
エラー訂正
S33
ヘッダー一致？
N
Y
S34
コンテンツ復号鍵を復号
S35
コンテンツを復号
S36
コンテンツ再生
エンド

【図１８】


差分集合への鍵割り当て
(疑似乱数生成器使用)
S41
各2分木のルートに
暗号(復号)鍵を割り当て
S42
ラベルを割り当て
S43
任意の部分木T_hを選択
S44
ノードviをルートとする
部分木$T_{h,i}$を選択
S45
差分集合$S_{i,*}$に暗号
(復号)鍵$L_{i,*}$を割り当て
S46
他の部分木
$T_{h,i}$あり?
Y
N
S47
他の部分木T_h
あり?
Y
N
リターン

【書類名】　要約書

【要約】

【課題】　記録媒体中の鍵情報量の増加を押さえつつ、再生装置の保有すべき秘密情報量を減少させることが可能な木構造を用いた鍵管理方式、及び、それを適用したコンテンツ記録／再生システムを提供する。

【解決手段】　情報提供者は、コンテンツを第１の暗号鍵により暗号化して暗号化コンテンツを生成するとともに、第１の暗号鍵に対応する第１の復号鍵を、第２の暗号鍵により暗号化して暗号化鍵情報を生成する。そして、暗号化コンテンツ及び暗号化鍵情報を記録媒体その他の形態で情報受信者に提供する。また、情報提供者は、予め第２の暗号鍵に対応する第２の復号鍵を生成するための情報を有しており、それを用いて第１の復号鍵を取得し、さらに第１の復号鍵を用いてコンテンツを復号化して再生することができる。第１の復号鍵及び第２の復号鍵は、情報受信者をリーフに割り当てた木構造を利用した鍵管理方式に基づいて情報受信者に配布される。ここで、上記木構造を複数の階層に分割して複数の部分木を規定し、部分木単位で鍵情報の割り当てを行うことにより、情報受信者が保有すべき鍵情報の情報量を減少させることができる。

【選択図】　図１

出証特２００３－３０５０５４０

出　願　人　履　歴　情　報

識別番号　　〔０００００５０１６〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都目黒区目黒１丁目４番１号
氏　名　パイオニア株式会社